LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

IPv6-VERKKOPALVELUT

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietotekniikka
Opinnäytetyö
Kevät 2013
Tiia Utti

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

UTTI, TIIA: IPv6-verkkopalvelut

Tietotekniikan opinnäytetyö, 53 sivua, 12 liitesivua

Kevät 2013

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli kehittää Lahden kaupungin langattoman verkon, Mastonetin, virtualisoidut verkkopalvelut toimimaan IPv6-protokollan kanssa. Mastonetin DHCP- ja DNS-verkkopalvelut on toteutettu alun perin Linux-palvelimille. Opinnäytetyön käytännön osuudessa toteutettiin vastaava ympäristö ja kehitettiin ympäristöä IPv6-yhteensopivaksi. Lisäksi samanlainen ympäristö rakennettiin käyttäen Windows-palvelimia. Lopuksi näitä kahta eri toteutusta verrattiin keskenään.

IPv6-protokollan käyttöönottoon on syytä valmistautua, koska IPv4-osoitteet eivät tule riittämään ikuisesti. Lisäksi IPv6 tuo parannuksia IPv4-protokollaan verrattuna. Tärkein parannus laajemman osoiteavaruuden lisäksi on tilaton autokonfiguraatio, jossa verkkoon liittyvä laite voi muodostaa itse verkkoon liittyessään itselleen IPv6-osoitteen.

IPv6-osoitteiden pituus tekee DHCP- ja DNS-verkkopalveluista entistä tärkeämmät. Se, että verkkoon liittyvä laite saa DHCP-palvelimelta IPv6-osoitetiedot tai käyttää osoitteen muodostamiseen tilatonta autokonfiguraatiota, muodostuu tärkeäksi kun on kyse 128 bitin pituisista IPv6-osoitteista. IPv6-osoitteiden pituus tekee osoitteiden ulkoa muistamisesta lähes mahdotonta. Tämän vuoksi IPv6-yhteensopiva DNS-nimipalvelu on toimivan verkon edellytys.

Opinnäytetyön käytännön osuudessa selvisi, että IPv6-verkkopalvelut ovat toteutettavissa Mastonetin käyttöön Linux-ympäristössä. Käytännön toteutuksen perusteella IPv6-ominaisuudet on mahdollista ottaa käyttöön myös Windows-palvelinympäristössä. Linux-palvelimilla käytetty DHCP-palvelinohjelmisto ei työn toteutusvaiheessa tarjonnut tukea DHCPv6:n failover-protokollalle. Tulevaisuudessa failover-protokollan tuki voi kuitenkin tuoda Linux-ympäristön vikasietoisuuden toteutukseen edun verrattuna Windows-ympäristöön.

Toteutuksien vertailussa todettiin Windows-ympäristön toteutus helpommaksi graafisen ympäristön vuoksi. Linux on kuitenkin palvelinkäytössä löytänyt oman vakaan asemansa. Työn perusteella voidaan todeta, että jos aikaisempi IPv4-palvelinympäristö on toteutettu Windows-palvelimilla, ei IPv6-ominaisuuksien käyttöönoton vuoksi ole tarpeellista vaihtaa toiseen palvelinympäristöön.

Asiasanat: IPv6, DNS, DHCP

Lahti University of Applied Sciences
Degree Programme in Information Technology

UTTI, TIIA: IPv6 network services

Bachelor’s Thesis in Information Technology, 53 pages, 12 pages of appendices

Spring 2013

ABSTRACT

The aim of this thesis was to develop the virtualized network services of Mastonet, the wireless network of the city of Lahti, to work with the IPv6 protocol. Mastonet's DHCP and DNS network services were originally developed to work on the Linux environment. In the practical part of the thesis the same environment was implemented with IPv6 support. Also, an identical environment was built by using Windows servers. Finally, these two implementations were compared.

The preparation for IPv6 deployment is necessary because the IPv4 address exhaustion will take place some day in the near future. Comparing to IPv4, IPv6 will bring improvements. The second most important improvement after larger address space is the stateless autoconfiguration. With stateless autoconfiguration the device entering the network will form the IPv6 address by itself.

The DHCP and DNS network services are more important with IPv6 because of the length of IPv6 addresses. The 128-bit-long IPv6 address means that it is important that the device gets the IPv6 address information from the DHCP server or by using stateless autoconfiguration. The length of the address will make memorizing the addresses almost impossible. That is the reason why the IPv6 compatible DNS name server is the prerequisite of a fully functional network.

In the practical part of the thesis it was found that the IPv6 network services can be implemented successfully to Mastonet's Linux environment. The practical implementation proved that the IPv6 features are also implementable to the Windows server environment. The DHCP server software used in the Linux environment did not support the DHCPv6 failover protocol at the time of the implementation. In the future the support of the failover protocol may bring the advantage of better fault tolerance on the Linux server environment than in the Windows server environment.

In the comparison of the two implementations it was found that the graphical user interface of the Windows environment facilitates the implementation of DHCP and DNS servers. However, Linux has gained a large share in server use. The practical implementation showed that the Windows server environment can be used with IPv6. From this it can be concluded that if the IPv4 server environment has been implemented with Windows servers, it is not necessary to change to another server environment because of IPv6.

Key words: IPv6, DNS, DHCP

SISÄLLYS

LYHENTEET

A	DNS:n tietuetyyppi, joka osoittaa IPv4-osoitteen.
AAAA	DNS:n tietuetyyppi, joka osoittaa IPv6-osoitteen.
BIOS	Basic Input / Output System. Tietokoneohjelma, joka lataa tarvittavat tiedot käyttöjärjestelmän käynnistymiseksi.
ccTLD	Country Code Top Level Domain. Maakohtainen ylimmän tason verkkotunnus nimipalvelujärjestelmän muodostamassa osoitehierarkiassa.
CIDR	Classless Inter-Domain Routing. Luokaton reititys, joka ilmoitetaan muodossa /x, jossa numero x kertoo kuinka monta bittiä osoitteen alusta kuuluu osoitteen verkko-osaan.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jota voidaan käyttää IP-osoitteen, oletusyhdyskäytävän ja nimipalvelimen jakamisessa lähiverkkoon kytkeytyville laitteille.
DHCPv6	Dynamic Host Configuration Protocol version 6. Verkkoprotokolla, jota voidaan käyttää IPv6-osoitteiden jakamisessa.
DMZ	Demilitarized Zone. Julkisille palveluille varattu verkko, josta tietoturvan nostamiseksi on rajoitettu liikennöintiä sisäverkkoon.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuntaa Internetin verkkotunnuksia IP-osoitteiksi.
DNS64	Domain Name System 64. DNS-palvelin, joka muodostaa IPv6-nimikyselyyn vastaukseksi IPv4-osoitteesta syntetisoidun IPv6-osoitteen.

FQDN	Fully Qualified Domain Name. Verkkotunnus, joka määrittelee tarkan sijainnin DNS-hierarkiassa.
gTLD	Generic Top Level Domain. Yleinen ylimmän tason verkkotunnus nimipalvelujärjestelmän muodostamassa osoitehierarkiassa.
IANA	Internet Assigned Numbers Authority. Taho, joka valvoo maailmanlaajuisesti IP-osoitteiden jakamista.
ICMP	Internet Control Message Protocol. Protokolla, jolla lähetetään viestejä koneesta toiseen, esimerkiksi virheviestejä.
IETF	Internet Engineering Task Force. Organisaatio, joka vastaa Internet-protokollien standardoinnista.
IPng	Internet Protocol Next Generation. IPv6:n nimi protokollan kehittämisen alkuvaiheessa.
IPsec	Internet Protocol Security. Kokoelma protokollia, joilla turvataan tietoliikenne IP-tasolla.
IPv4	Internet Protocol version 4. Internet-protokollan neljäs versio.
IPv6	Internet Protocol version 6. Internet-protokollan kuudes versio.
NAT	Network Address Translation. Osoitteenmuunnostekniikka, jonka avulla useampi kone liikennöi yhdellä IP-osoitteella.
NAT64	Network Address Translation 64. Mekanismi, jonka avulla IPv6-laitteet voivat kommunikoida IPv4-palvelimien kanssa.
NTP	Network Time Protocol. Protokolla, joka mahdollistaa tietokoneen ajan synkronoimisen.

PTR	Pointer Record. DNS:n tietuetyyppi, joka osoittaa IPv4- tai IPv6-osoitteen nimen.
RA	Router Advertisement. Reitittimen lähettämä viesti, jolla se mainostaa itseään verkkoon.
RFC	Request for Comments. IETF-organisaation julkaisemia asiakirjoja, jotka sisältävät kuvauksia Internetin erilaisista käytännöistä, protokollista.
TCP/IP	Transmission Control Protocol / Internet Protocol. Internet-liikennöinnissä käytettävien tietoverkkoprotokollien yhdistelmä.
TLD	Top Level Domain. Ylätason verkkotunnus nimipalvelujärjestelmän muodostamassa osoitehierarkiassa.
TTL	Time to Live. Määrittelee DNS:ssä toimialuetiedoston säilytysajan tallentavassa nimipalvelimessa.
UDP	User Datagram Protocol. Yhteydetön protokolla, jonka avulla voidaan siirtää tiedostoja.

1 JOHDANTO

1.1 Työn tausta

Mastonet on Lahden kaupungissa toimiva ilmainen langaton verkko. Verkko kattaa kaupungin niin sanotut HotSpot-pisteet eli tärkeimmät sijainnit, joita ovat esimerkiksi kirjastot ja rautatieasema. Tärkeimpien sijaintien lisäksi Mastonet on suunniteltu palvelemaan tärkeimpien tapahtumien vieraita. Tällainen tapahtuma on esimerkiksi Lahdessa vuosittain järjestettävä Salpausselän kisat.

Mastonetin ylläpidosta on vastannut vuodesta 2009 lähtien Lahden ammattikorkeakoulu. Lahden ammattikorkeakoulussa verkkoa kehitetään osana tietotekniikan insinööriopintoja. Tämä opinnäytetyö vastaa verkon kehittämistarpeisiin IPv6-protokollan osalta.

1.2 Työn tavoitteet

Tämän opinnäytetyön tavoitteena on kehittää Mastonetin virtualisoituja verkkopalveluja toimimaan IPv6-protokollan kanssa. Mastonetin verkkopalvelut sisältävät DHCP- ja DNS-palvelimet, jotka on suunniteltu toimimaan IPv4-protokollan kanssa. Tavoite on saada samat palvelut toimimaan myös IPv6:n kanssa.

Mastonetin verkkopalvelut ovat entuudestaan kahdennettuja. Tämä tarkoittaa sitä, että ensisijaisen palvelimen vikaannuttua, on olemassa toinen palvelin, joka toimii ensisijaisen palvelimen sijasta vikatilanteessa. Kahdennetut verkkopalvelut on tarkoitus saada toimimaan myös IPv6:n kanssa. Toteutus tapahtuu virtualisoituna mukaillen aikaisempaa toteutusta.

Virtualisoidut IPv6-verkkopalvelut toteutetaan Linux-palvelinten lisäksi myös Windows-palvelimilla. Kahden eri ympäristön toteutuksia on tarkoitus vertailla. Toteutuksissa keskitytään siihen, miten IPv6-ominaisuudet toteutetaan. Näin ollen tässä työssä ei käydä läpi kaikkia ominaisuuksia, jotka palvelinkäytössä ovat hyödyllisiä konfiguroida palvelimiin.

2 IPv6-PROTOKOLLA

2.1 Yleistä IPv6-protokollasta

IPv6:n (Internet Protocol version 6) alkutaival alkoi vuonna 1992, jolloin Internet Engineering Task Force (IETF) ymmärsi IPv4-osoitteiden riittämättömyyden ja protokollan tekniset rajoitukset uusien protokollien käyttöönotossa (Hagino 2005, 1). Tuolloin IETF aloitti työskentelyn IPv4-protokollan seuraajan kehittämiseksi. Uutta protokollaa kutsuttiin kehityksen alkuvaiheessa nimellä Internet Protocol Next Generation (IPng), jonka toiminnallisuuksiksi tutkittiin erilaisia ehdotuksia ja suosituksia. IPv6:n toteuttamista ehdotettiin vuonna 1994 IETF:n Toronton kokouksessa. Ehdotus on määritelty RFC (Request For Comments) 1751 -dokumentissa. Samana vuonna IETF perusti ryhmän määrittämään IPv4:n arvioidun eliniän. Tämän elinikäarvion perusteella nähtiin se onko aikaa kehittää uuteen protokollaan uusia toiminnallisuuksia vai onko tarve ensimmäiseksi luoda ainoastaan suurempi osoiteavaruus. (Hagen 2006, 3.)

IPv6:n kehittäjäryhmä on IP-osoiteavaruuden laajentamisen lisäksi myös tehnyt uuteen protokollaan muita muutoksia verrattuna IPv4:ään. Tästä huolimatta laajempi osoiteavaruus on uuden protokollan tärkein ominaisuus. IPv4 mahdollistaa teoriassa ainoastaan noin neljä miljardia (2^{32}) IP-osoitetta, mutta käytännössä mahdollisten osoitteiden määrä on pienempi. Lisäksi IPv4-osoitteiden alkuvaiheilla käytetyt osoitteiden jakamisen tavat eivät olleet tehokkaita. Tämän vuoksi joidenkin organisaatioiden käyttöön on annettu suurempia osoitelohkoja kuin ne tarvitsisivat. Tämä on vähentänyt vapaiden IP-osoitteiden määrää huomattavasti. Myös tekniikan kehittyminen on lisännyt tarvittavien IP-osoitteiden määrää. Jo 1994 IETF:n perustama työryhmä ennusti silloisten tilastojen avulla IPv4-osoitteiden loppumisen tapahtuvan vuosien 2005 ja 2011 välillä. (Hagen 2006, 3, 5.) Vuonna 2011 IPv4-osoitteiden loppumisesta uutisoitiin laajasti Suomenkin tiedotusvälineissä. Osoitteiden loppumisen uutisoitiin hidastavan Internetin toimintaa. Osoitteiden loppumista vastaan kuitenkin on käytetty osoitteenmuunnosta (NAT, Network Address Translation), koska IPv6:een siirtymisen heikkoutena on ollut siirtymiskustannukset. (Heikkilä 2011; Roivas 2011.)

2.2 Nykytilanne

IPv6:n nykytilanteen kannalta tärkeimpiä ovat olleet viime vuosina järjestetyt kaksi tapahtumaa. Tapahtumien tarkoitus on ollut edistää IPv6:n käyttöön ottamisen prosessia. Näistä ensimmäinen tapahtuma oli 8.6.2011 vietetty IPv6-päivä (World IPv6 Day). Päivän aikana useat sivustot ja organisaatiot ottivat IPv6-tuen käyttöön 24 tunnin ajaksi. Mukana oli myös suuria Internetin palveluja kuten Google ja Facebook sekä suuria organisaatioita kuten Microsoft. Suomessa päivään osallistuivat esimerkiksi Iltalehti ja MTV3. Yhteensä mukana oli yli 400 organisaatiota. Päivän aikana verkkopalveluiden nimipalvelimet tarjosivat IPv6-osoitteita, mikäli IPv6-tekniikka oli tuettu käyttäjän laitteella. IPv4-tekniikkaa käyttävät ohjattiin IPv4-osoitteisiin. IPv6-päivä onnistui järjestäjien mukaan hyvin. Hankaluuksia yksittäisille käyttäjille saattoi kuitenkin aiheutua väärin toimivista verkkolaitteista, esimerkiksi laajakaistareitittimestä. Tällaisessä tilanteessa IPv6-tekniikka tuli käyttöön vaikka itse laite ei sitä tukenutkaan. (Laitila 2011; Lehto 2011; Kotilainen 2011.)

Toinen tapahtuma seurasi vuoden päästä IPv6-päivää. Tämä tapahtuma oli 6.6.2012 järjestetty World IPv6 Launch, jolloin suurimmat verkkopalvelut, kuten Google ja Facebook, ottivat IPv6-tekniikan pysyvästi käyttöön. IPv4 jäi kuitenkin toimimaan IPv6:n rinnalle näissä palveluissa, kuten se oli toiminut IPv6-päivän aikana. Kotikäyttäjille tämä kesäkuun 2012 muutos ei välttämättä näkynyt millään tavalla, mitä voidaan pitää hyvänä merkkinä siitä, että IPv6:een siirtyminen on toteutettavissa onnistuneesti. IPv4 tulee kuitenkin näissä ja myöhemmin IPv6-tekniikkaan siirtyvissä palveluissa toimimaan pitkään rinnalla. Se, miten pitkään IPv4 ja IPv6 toimivat rinnakkain, on tässä vaiheessa vielä vain arvailujen varassa. (Kotilainen 2012.)

2.3 Edut

IETF ei kehittäessään protokollaa lisännyt ainoastaan osoitteiden määrää vaan kiinnitti huomiota myös IPv4:n puutteisiin. Näin ollen IPv6 tuo etuja, joita IPv4 ei voi tarjota. Näistä tärkeimmät ovat laajempi osoiteavaruus ja tilaton autokonfiguraatio. Näiden lisäksi IPv6 tuo muitakin muutoksia IPv4:ään

verrattuna. Tässä luvussa käydään läpi kaksi tärkeintä IPv6:n tuomaa uudistusta sekä muita IPv6:n tuomia etuja. (van Beijnum 2006, 2-3.)

2.3.1 Laajempi osoiteavaruus

Laajempi osoiteavaruus on IPv6-protokollan selkein ja tärkein etu. IPv4-osoitteen 32 bitin sijasta IPv6-osoite käyttää osoitteeseen 128 bittiä. Tämä mahdollistaa teoriassa noin $3{,}4 \times 10^{38}$ yksittäistä osoitetta. Mahdollisten IPv6-osoitteiden määrän suuruutta havainnollistaa se, että osoitteita riittäisi jokaiselle hiekanjyvälle maapallolla. Mahdollisten IPv6-osoitteiden määrän suuruutta havainnollistaa myös vertailu mahdollisten IPv4- ja IPv6-osoitteiden lukumäärien kesken.

4 294 967 296
340 282 366 920 938 463 463 374 607 431 768 211 456

Ylempi luku kuvaa mahdolliset IPv4-osoitteet ja alempi vastaavasti mahdolliset IPv6-osoitteet. (van Beijnum 2006, 2; Hagen 2006, 3.)

IPv6-osoiteavaruuden laajuus mahdollistaa erilaisten mobiiliteknologioiden käyttöönottamisen. Pysyviä IP-osoitteita voidaan tarvita esimerkiksi autojen ja muiden elektronisten laitteiden seurantaan ja ylläpitoon. Suurimmat autonvalmistajat, esimerkiksi Renault, ovat ottaneet teknologian omakseen uusien automallien suunnittelussa. (Hagen 2006, 36.) Osoitteiden lukumäärän lisäämisen lisäksi IPv6:ssa on käytetty uuden protokollan suunnittelun tuoma mahdollisuus myös osoitearkkitehtuurin kehittämiseen. IPv6-osoitteita tarkastellaan tarkemmin luvussa 3. (Loshin 2004, 124.)

2.3.2 Autokonfiguraatio

IPv6 tukee sekä tilallista että tilatonta osoitteiden autokonfiguraatiota. Tilallisessa autokonfiguraatiossa (stateful autoconfiguration), jota myös IPv4 tukee, käytetään IPv6:ssa osoitteiden jakamiseen DHCPv6-palvelinta. Palvelin jakaa osoitteita verkkoon liittyville laitteille ja ylläpitää tietoa jaetuista osoitteista. Uutena ominaisuutena IPv6 tuo tilattoman autokonfiguraation (stateless autoconfiguration), jossa laite muodostaa itselleen osoitteen käyttäen tietoa, jonka

reititin on mainostanut verkossa. Verkon laitteet voivat käyttää molempia tapoja, tilatonta ja tilallista, yhtä aikaa. (Youngsong & Hyewon 2005, 74; van Beijnum 2006, 3.)

Tilattomassa autokonfiguraatiossa laitteen osoite muodostuu kahdessa osassa. Ensimmäiset 64 bittiä IPv6-osoitteesta ovat reitittimen laitteelle mainostamat. Kaikilla samaan verkkoon liittyvillä nämä 64 bittiä ovat samat. Osoitteen loput 64 bittiä muodostuvat laitteen verkkoliitännän MAC-osoitteen perusteella. Näin ollen jokaisella verkon laitteella on oma uniikki 128-bittinen IPv6-osoite. Tilaton autokonfiguraatio mahdollistaa myös sen, että jokainen verkon laite saa aina samaan verkkoon liittyessä saman osoitteen ilman manuaalista konfigurointia. (van Beijnum 2006, 3.)

2.3.3 Muita etuja

Tässä alaluvussa mainitaan vielä joitakin IPv6:n tuomia etuja tai muutoksia. Tällainen etu on esimerkiksi IPv6:n tilattoman autokonfiguraation useiden laitteiden IPv6-osoitteiden muuttaminen yhtä aikaa. Reitittimen tarvitsee ainoastaan lopettaa vanhan verkko-osan mainostaminen ja aloittaa uuden verkko-osan mainostus. Tämän jälkeen verkon laitteet muodostavat automaattisesti uuden IPv6-osoitteen verkkoliitännälleen. Osoitteiden lennossa muuttaminen ei kuitenkaan laske verkon toimintaa, koska vanhat osoitteet toimivat olemassa olevissa yhteyksissä. Uusien yhteyksien muodostuksissa käytetään kuitenkin uusia laitteiden muodostamia osoitteita. (van Beijnum 2006, 4.)

IPv6:n etuna on myös tehokkuus. IPv6 on kehitetty IPv4:ää tehokkaammaksi muun muassa seuraavilla tavoilla.

- IPv6:n otsikkokenttä on kiinteä pituudeltaan.
- IPv6-otsikkokenttä on optimoitu prosessoitavaksi jopa 64 bittiä kerrallaan. IPv4:ssä tämä oli vain 32 bittiä.
- IPv4:n otsikkokentän joka kerta reitittimen jälkeen laskettava tarkistussumma on poistettu IPv6:sta.

- Reititin voi pyytää lähdettä lähettämään liian suuret paketit uudestaan pienemmissä paketeissa. Reitittimen ei enää tarvitse muuttaa itse pakettia pienemmiksi palasiksi.
- Broadcast-toiminnot ovat IPv6:ssa korvattu multicastilla. Näin ollen vain multicastia kuuntelevat laitteet saavat viestit kun taas broadcast-toiminnossa viestit menivät myös päätelaitteille.

(van Beijnum 2006, 4.)

IPv6:n sanominen IPv4:ää turvallisemmaksi sen takia, että siihen on määritelty IPsec-tuki pakolliseksi, voidaan laskea myytiksi. IPsec on kuitenkin ollut käytettävissä myös IPv4-toteutuksiin. IPsec tarjoaa IP-tason autentikaatiota ja salausta. Kummankin protokollan osalta IPsec vaatii kuitenkin edistynyttä konfigurointia. (van Beijnum 2006, 4.)

3 IPv6-OSOITTEET JA IPv6-PAKETIN RAKENNE

3.1 IPv6-osoitteet

3.1.1 Osoitteiden rakenne ja aliverkotus

128-bittinen IPv6-osoite jakautuu kahdeksaan eri osaan. Jokainen osa on 16 bittiä ja osat ilmaistaan neljällä heksadesimaalilla. Jokainen 16 bitin lohko erotetaan toisistaan kaksoispisteellä. IPv6-osoitteen muoto on siis esimerkiksi seuraavanlainen.

2001:0708:0410:0003:0000:0000:0000:0001

IPv6-osoitteen saman lohkon peräkkäiset nollat voidaan ilmaista pelkästään yhdellä nollalla tai jättää kokonaan pois lohkon alusta. Näin ollen edellisen IPv6-osoite-esimerkin loppuosan nollia sisältävät lohkot voitaisiin esittää jokainen vain yhdellä nollalla. IPv6-osoite on mahdollista kirjoittaa vieläkin yksinkertaisemmassa muodossa. Lohkot, joissa on nolla-arvoja, voidaan korvata kahdella kaksoispisteellä. Oli sitten kyseessä vain yksi lohko nolla-arvoilla tai esimerkiksi kolme peräkkäistä lohkoa nolla-arvoilla, voi kummassakin tapauksessa kirjoittaa näiden nolla-arvon sisältävien lohkojen tilalle kaksi kaksoispistettä. Tämän voi kuitenkin tehdä vain yhdessä kohtaa IPv6-osoitetta. Näin ollen ylemmän esimerkin IPv6-osoite voidaan kirjoittaa seuraavassa muodossa.

2001:708:410:3::1

Taulukko 1 esittää muuntotaulukon binääri-, heksadesimaali ja desimaalimuotojen välillä. (Davies 2012, 58-60.)

TAULUKKO 1. Muuntotaulukko binääri-, heksadesimaali- ja desimaalimuotojen välillä (Davies 2012, 59)

Binary	Hexadecimal	Decimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

Aliverkotus ilmoitetaan IPv6:ssa CIDR-notaatiolla (Classless Inter-Domain Routing). Tämä tarkoittaa sitä, että IPv6-osoitteen perässä ilmoitetaan aliverkon peite. Aliverkon peite ilmoitetaan desimaalimuodossa ja erotetaan IPv6-osoitteesta kauttaviivalla. 64-bittistä aliverkon peitettä käytetään yksittäisissä verkoissa, jotka ovat kiinni solmuissa (node). Esimerkki IPv6-osoitteesta aliverkon peitteen kanssa on seuraavanlainen.

2001:708:410:3::1/64

Esimerkin osoitteen verkko-osa, prefix, on täten 2001:708:410:3::/64. (Davies 2012, 60.)

Taulukko 2 esittää listan määrätyistä prefixeistä ja erikoisosoitteista. Listan ulkopuolelle jäävät osoitteet voivat olla tällä hetkellä varattuja tai jakamattomia. Ajantasaisimman tiedon osoitteiden jaosta kertoo IANAn (Internet Assigned Numbers Authority) www-sivut osoitteessa

http://www.iana.org/assignments/ipv6-address-space. Taulukon binäärimuotoisen prefixin 0000 0000 osoitteista osa on rajattu erikoisosoitteiksi. Nämä ovat määrittelemätön osoite (unspecified address), loopback-osoite ja IPv6-osoitteet, joihin on sisällytetty IPv4-osoite. (Hagen 2006, 39-40.)

TAULUKKO 2. Lista määrätyistä, allokoiduista, prefixeistä (Hagen 2006, 39)

Allocation	Prefix binary	Prefix hex	Fraction of address space
Unassigned	0000 0000	::0/8	1/256
Reserved	0000 001		1/128
Global unicast	001	2000::/3	1/8
Link-local unicast	1111 1110 10	FE80::/10	1/1024
Reserved (formely Site-local unicast)	1111 1110 11	FEC0::/10* * deprecated	1/1024
Local IPv6 address	1111 110	FC00::/7	
Private administration	1111 1101	FD00::/8	
Multicast	1111 1111	FF00::/8	1/256

Määrittelemätön osoite 0:0:0:0:0:0:0:0, joka voidaan myös ilmaista ::, kertoo sen, että validia IPv6-osoitetta ei ole. Tällaistä osoitetta ei kuitenkaan saa missään tilanteessa määrittää staattisesti tai dynaamisesti millekään verkkoliitännälle. Loopback-osoite ::1 tarkoittaa samaa kuin IPv4:ssä osoite 127.0.0.1. Loopback-osoitetta voi käyttää vianetsinnässä ja testauksessa, koska tämä osoite ei lähetä paketteja eteenpäin. Myöskään loopback-osoitetta ei saa määrittää millekään verkkoliitännälle. (Hagen 2006, 44.)

3.1.2 Osoitetyypit

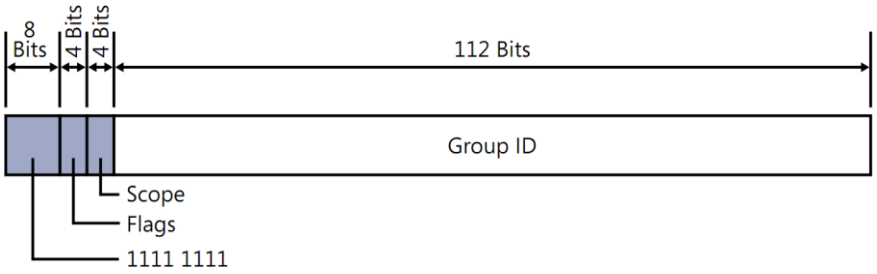
IPv6-osoitteita on kolmea eri tyyppiä. Nämä tyypit ovat unicast, multicast ja anycast. Uudistus IPv4:ään verrattuna on broadcast-osoitteiden poistuminen. Lisäksi IPv6:n kanssa on todennäköistä, että anycast-osoitetta tullaan käyttämään laajemmin kuin IPv4:n kanssa. (Hagen 2006, 36.)

Unicast-osoite yksilöi verkkoliitännän. Paketti, joka on osoitettu unicast-osoitteeseen, toimitetaan siihen verkkoliitäntään, jonka kyseinen osoite yksilöi. (Hagen 2006, 36.) Unicast-osoitteita on eri tyyppejä, joita ovat

- globaalit unicast -osoitteet (global unicast addresses),
- link-local-osoitteet,
- unique local -osoitteet,
- erikoisosoitteet (special addresses) ja
- ns. siirtymisosoitteet (transition addresses).

Globaalit unicast-osoitteet ovat reititettävissä ja tavoitettavissa Internetissä eli ne vastaavat IPv4:n julkisia IP-osoitteita. Link-local-osoitteita käytetään yksittäisessä aliverkossa laitteiden välisessä kommunikoinnissa. Link-local-osoitteita ei ole mahdollista reitittää edes yksityisen verkon sisällä. IPv6:n link-local-osoitteita voi verrata IPv4:n link-local-osoitteisiin 169.254.0.0/16. Kuten taulukosta 2 selviää, on link-local-osoitteiden prefix fe80::/10. Link-local-osoite muodostetaan automaattisesti verkkoliitännälle ja sen loppuosa koostuu yleensä MAC-osoitteesta. Unique local -osoitteiden prefix on FC00::/7 ja ne ovat yksityisiä osoitteita, jotka eivät ole reititettävissä Internetissä. Link-local-osoitteista poiketen unique local -osoitteet ovat aina yksilöllisiä kun taas link-local-osoitteita voi olla samoja eri aliverkoissa. Erikoisosoitteet ovat määrittelemätön osoite ja loopback-osoite, jotka selvitettiin edellisessä luvussa. Lisäksi niin sanotuissa siirtymisosoitteissa IPv4-osoite on jollakin tekniikalla sisällytetty IPv6-muotoisiin osoitteisiin. (Davies 2012, 62, 65-68.)

Multicast-osoitteet ovat ryhmäosoitteita eli multicast-osoitteeseen lähetettävät paketit menevät kaikille kyseisen multicast-ryhmän jäsenille. Multicast-osoitteiden alku on aina FF, jonka jälkeen osoitteessa on ilmoitettu liput (flags), scope ja ryhmä-ID. Multicast-osoitteen rakennetta selventää kuvio 1. Scope määrittää sen, miten laajasti multicast-lähetys on tarkoitettu lähetettäväksi, esimerkiksi vain kyseiseen solmuun tai globaalisti. Vaihtoehtoja lähetyksen laajuudeksi on useita. Ryhmä-ID kertoo multicast-ryhmän, jolle paketit ovat tarkoitettu. (Davies 2012, 68-69.)



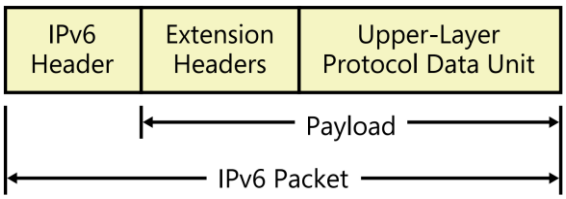
KUVIO 1. IPv6 multicast-osoitteen rakenne (Davies 2012, 69)

Anycastin toiminta on samantapainen kuin multicastin. Eroavaisuus on kuitenkin siinä, että anycast-osoitteeseen lähetetty paketti toimitetaan vain yhdelle anycast-ryhmän jäsenelle. Se ryhmän jäsen, jolle paketti toimitetaan, määräytyy reititystietojen mukaan. Reititystietojen mukaan valitaan lähin kohteista. (van Beijnum 2006, 15.) Anycast-osoitteet on suunniteltu tuomaan vikasietoisuutta ja kuormantasausta ympäristöissä, joissa samaa palvelua ylläpidetään useammissa palvelimissa tai reitittimissä. Tällaisia palveluja ovat esimerkiksi DNS ja HTTP. (Hagen 2006, 50.)

3.2 IPv6-paketin rakenne

3.2.1 Paketin rakenne

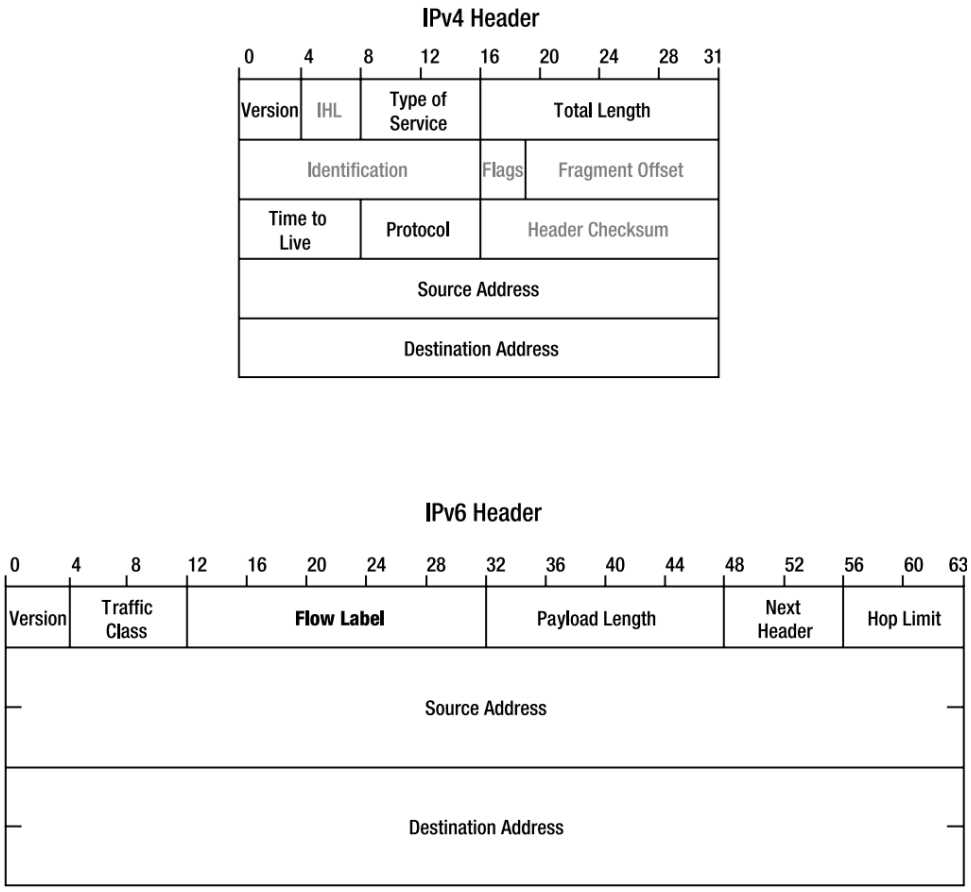
IPv6-paketin rakenne selviää kuviosta 2. Paketti koostuu IPv6-otsikkokentästä, laajennusotsikoista ja ylemmän tason kuljetustiedoista. IPv6-otsikkokenttä on aina pituudeltaan 40 tavua. Otsikkokentän sisältö kuvataan tarkemmin seuraavassa luvussa. IPv6-paketissa voi olla laajennusotsikoita. Ylemmän tason kuljetustiedot voivat sisältää esimerkiksi ylemmän tason otsikon ja tiedon kuorman määrästä. (Davies 2012, 91-92.)



KUVIO 2. IPv6-paketin rakenne (Davies 2012, 91)

3.2.2 IPv6-otsikko

IPv6-otsikko on pituudeltaan 40 tavua kun taas IPv4-otsikon pituus voi vaihdella 20 tavusta 60 tavuun. Näin ollen IPv4-otsikossa piti määrittää se, mikä on otsikon kokonaispituus (header length). Tämä kenttä on yksi viidestä kentästä, joita ei IPv6-otsikosta löydy. Kuviosta 3 selviää IPv4- ja IPv6-otsikoiden kentät. IPv4-otsikon rakennetta kuvaavassa kuvassa on merkitty harmaaksi ne kentät, joita ei IPv6-otsikosta löydy. (Hagen 2006, 17.)



KUVIO 3. IPv4- ja IPv6-otsikot (van Beijnum 2006, 152)

Poistuneiden kenttien lisäksi joidenkin kenttien nimet ja tarkoitukset ovat osittain muuttuneet. Tällaisiä kenttiä ovat Type of Service (IPv6: Traffic Class), Total Length (IPv6: Payload Length) ja Time to Live (IPv6: Hop Limit). Kentät Identification, Flags ja Fragment Offset liittyivät pakettien pienemmiksi paketeiksi muuttamiseen reitittimissä mikäli kohdeverkko tukee ainoastaan pienempiä paketteja. IPv6 ei tue pakettien fragmentaatiota reitittimissä vaan pakettien fragmentointi tapahtuu lähettävässä laitteessa. Tämän vuoksi pakettien fragmentointiin liittyvät kentät on poistettu. Fragmentointimääritykset annetaan tarvittaessa laajennusotsikoissa. Header checksum -kenttä on poistettu paketin käsittelynopeuden nostamiseksi. Näin ollen reitittimen ei tarvitse laskea ja päivittää otsikon tarkistussummaa. (van Beijnum 2006, 152-153; Hagen 2006, 18.)

3.2.3 Lisäotsikot

IPv6-paketti sisältää lisäotsikoita, koska IPv6-otsikon pituus on aina 40 tavua. Näin ollen IPv6-otsikkoon ei voi lisätä vaihtuvia määrittelyitä. Yleisimmät lisäotsikot ovat seuraavat.

- Hop-by-Hop Options
- Routing
- Fragment
- Authentication
- Encapsulating Security Payload (ESP)
- Destination Options

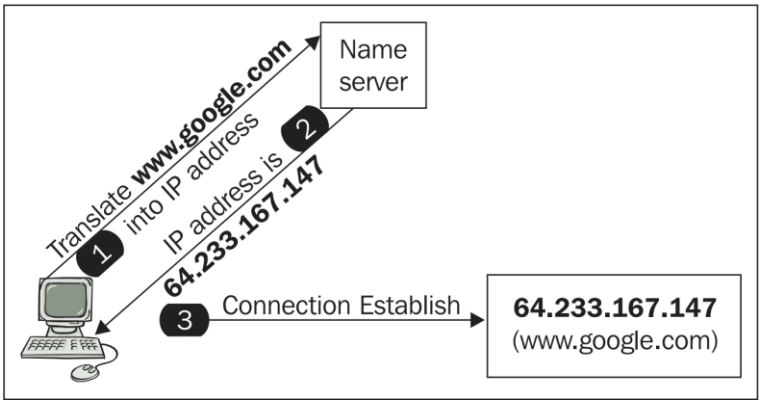
Se, ovatko lisäotsikot käytössä, määritellään IPv6-otsikon Next Header -kentässä eli seuraavan otsikon määrittävässä kentässä. (van Beijnum 2006, 155.)

Lisäotsikot käsitellään vasta kohteessa. Poikkeus tähän on kuitenkin Hop-by-Hop Options -kenttä, joka käsitellään jokaisessa solmussa paketin reitin varrella. Tämän vuoksi kyseisen kentän pitää sijaita heti IPv6-otsikon jälkeen. (Hagen 2006, 23.)

4 DNS JA IPv6

4.1 DNS yleisesti

DNS (Domain Name System) on nimipalvelujärjestelmä, jonka avulla IP-osoitteiden sijasta on mahdollista käyttää selväkielisiä nimiä. Järjestelmä mahdollistaa verkkotunnusten käyttämisen kaikkien komentojen yhteydessä, missä käytettäisiin IP-osoitetta. Poikkeus tähän on kuitenkin nimipalvelimen määritys, joka tehdään käyttäen IP-osoitetta. IP-osoitteiden ja verkkotunnuksien suhteiden määritys tapahtuu DNS-tietokannoissa. Kuvio 4 havainnollistaa DNS:n toimintaa otettaessa yhteyttä Google-hakupalvelun www-osoitteeseen. Ennen kuin yhteys www.google.com-palvelimeen muodostuu, nimipalvelin muuntaa DNS-nimen IP-osoitteeksi. (Dostálek & Kabelová 2006, 5.)



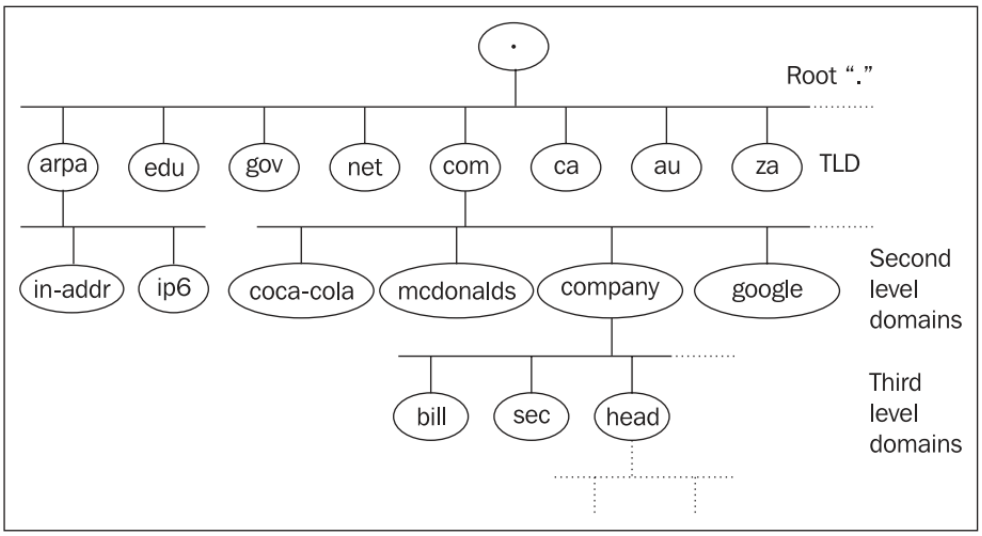
KUVIO 4. Nimipalvelujärjestelmän toimintaperiaate (Dostálek & Kabelová 2006, 5)

IPv6 nostaa DNS:n jopa aikaisempaa tärkeämmäksi IPv6-osoitteiden pituuden vuoksi. Käyttötarkoitukseltaan DNS on IPv6:n kanssa samanlainen kuin IPv4:n eli verkkotunnuksen ja IP-osoitteen yhdistäminen toisiinsa. IPv6:n käyttäminen varsinkin yhtä aikaa IPv4:n kanssa tuo kuitenkin muutoksia nimipalvelujärjestelmään toiminnan takaamiseksi. (Hagen 2006, 242.)

4.2 Verkkotunnuksien muodostuminen

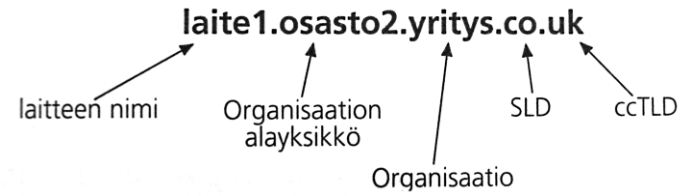
Internet on jaettu eri verkkotunnuksiin, domaineihin, jotka määrittelevät loogisesti yhteenkuuluvat nimet. Verkkotunnuksista selviää kuuluuko tietty nimi esimerkiksi maalle tai yritykselle. Verkkotunnuksia on mahdollista jakaa myös aliosoitteisiin. Tätä voidaan käyttää esimerkiksi yrityksien kohdalla, jolloin on mahdollista antaa esimerkiksi eri yksiköille oma aliosoite yrityksen verkkotunnuksen alle. (Dostálek & Kabelová 2006, 6.)

Verkkotunnus muodostuu merkkijonoista, jotka on eroteltu pistein. Verkkotunnuksen käsittely tapahtuu vasemmalta oikealle. Kuvio 5 esittelee nimipalvelujärjestelmän muodostaman osoitehierarkian, ylösalaisin käännetyn puun, puumallin. Korkeimmalla hierarkiassa on juuri, joka esitetään pisteenä. Verkkotunnuksessa tämä piste olisi oikealla viimeisenä, tämä piste jätetään kuitenkin yleensä kirjoittamatta. Juurta seuraavana ovat ylätason verkkotunnukset (TLD, Top Level Domain), joita on kahta eri tyyppiä. Nämä ovat gTLD (Generic Top Level Domain) ja ccTLD (Country Code Top Level Domain). ccTLD-nimet kattavat eri maille määritellyt kaksikirjaimiset verkkotunnukset, esimerkiksi Suomen ccTLD on fi. gTLD-nimistä hyvin tunnettuja ovat esimerkiksi edu, com ja net. (Dostálek & Kabelová 2006, 6.) Ylätason verkkotunnuksien alla, seuraavalla tasolla, sijaitsevat SLD-nimet (Second Level Domain), jotka voivat tarkentaa esimerkiksi maatunnuksen sisällä kaupallisessa käytössä olevat verkkotunnukset. Tunnetuin esimerkki on tästä Iso-Britannian co.uk, jonka tunnus kattaa kaupallisessa (commercial) käytössä olevat verkkotunnukset. Toinen vaihtoehto SLD-nimelle on esimerkiksi yritys, yhteisö tai tuotemerkki. (Anttila 2000, 233, 235.) Osoitteesta muodostuu FQDN (Fully Qualified Domain Name), kun osoite päättyy pisteeseen. Esimerkiksi laite.yritys.fi. on FQDN. Osoitteen päättyessä pisteeseen, osoitteen oletetaan olevan tarkka. Tätä yleensä käytetään tilanteissa, joissa halutaan varmistaa, että osoitteen perään ei lisätä enää muita merkkejä, esimerkiksi osoitteen verkko-osaa .yritys.fi. (Britt, Davis, Forrester, Liu, Matthews, Parziale, Rosselot 2006, 428.)



KUVIO 5. Nimipalvelujärjestelmän osoitehierarkia/puumalli (Dostálek & Kabelová 2006, 7)

Yrityksen käytössä olevaan verkkotunnukseen, esimerkiksi yritys.fi, on mahdollista tehdä aliverkkotunnuksia eri käyttötarkoituksia varten. Esimerkiksi yrityksen rekrytointiosaston käytössä voi olla rekrytointi.yritys.fi. Kuten kuvio 5 osoittaa, voi verkkotunnuksen muodostuminen jatkua käyttötarkoituksesta riippuen vielä tasoja alaspäin. (Dostálek & Kabelová 2006, 6.) Kuviosta 6 selviää, miten laitteen nimi muodostuu. Kuvan laitteen nimessä ccTLD-nimi on uk eli Iso-Britannian maatunnus. SLD-nimi on esimerkissä co eli kyseessä on kaupallisessa tarkoituksessa oleva verkkotunnus. Ennen SLD-nimeä esimerkissä on aliverkkotunnus yritykselle ja tätä ennen on määritelty yrityksen osasto. Ensimmäisenä on määritelty laite. Näin esimerkissä määrittyy laitteen verkkonimi. (Anttila 2000, 233.)



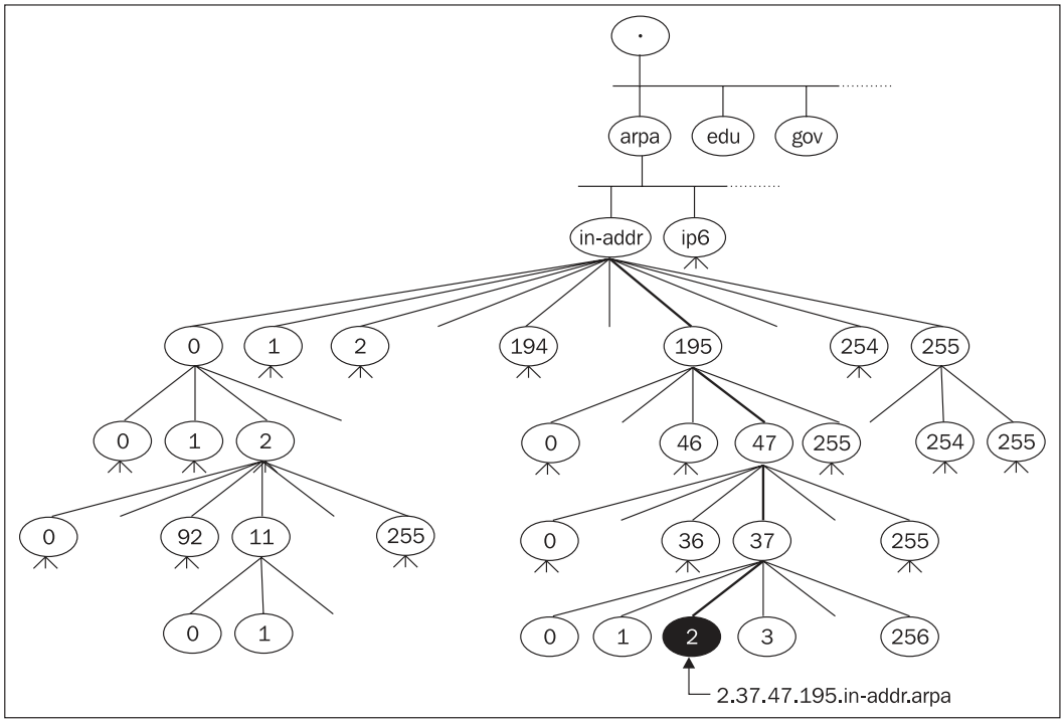
KUVIO 6. Laitteen verkkonimen muodostuminen (Anttila 2000, 233)

4.3 Toiminta ja viestiliikenne

DNS-järjestelmässä on kolmea eri tyyppiä nimipalvelimia, jotka ovat päänimipalvelin (primary), sekundäärinimipalvelin (secondary) ja tallentava nimipalvelin (caching-only). Päänimipalvelimia on yksi kappale jokaisella toimialueella. Poikkeus tähän on kuitenkin juuritaso. Juuritasolla nimipalvelimia on 13 kappaletta ja ne sijaitsevat ympäri maailmaa. Päänimipalvelin ylläpitää toimialueen tietoja, jotka käytännössä ovat tiedostoja. Näitä kutsutaan aluetiedostoiksi, zone-tiedostoiksi. Päänimipalvelin voi vastata useammasta toimialueesta. Sekundäärinimipalvelimien eli varanimipalvelimien tehtävä on nimensä mukaisesti olla varanimipalvelin päänimipalvelimen ollessa pois käytöstä. Varanimipalvelin kopioi zone-tiedostot päänimipalvelimelta tietyin väliajoin ja näin ollen varanimipalvelin sisältää samat zone-tiedot kuin päänimipalvelin. Tallentava nimipalvelin tallentaa tiedot pää- tai varanimipalvelimelta ja säilyttää ne zone-tiedostojen TTL-kentässä (Time To Live) määritetyn ajan verran. Tämän jälkeen tiedot poistetaan tallentavasta nimipalvelimesta. Siihen asti tiedot ovat käytettävissä esimerkiksi tilanteissa, joissa pää- ja varanimipalvelimia ei haluta kuormittaa kaikilla nimikyselyillä. (Anttila 2000, 239-242.)

Nimipalvelun toimimiseksi työasemasta pitää löytyä resolveri. Resolveri on ohjelmakomponentti, joka käsittelee nimikyselyiden verkkonimen tai IP-osoitteen kääntämiseen vaadittavat tehtävät. Käytännössä resolverin tehtävä on lähettää nimikysely DNS-palvelimeen ja käsitellä sieltä tuleva vastaus. (Anttila 2000, 243.)

IP-osoitteen selvittämistä osoitteesta kutsutaan forward-nimipalveluksi. Vastaavasti nimipalvelin pystyy selvittämään laitteen nimen IP-osoitteen perusteella. Tätä kutsutaan reverse-nimipalveluksi, käänteiseksi nimipalveluksi. (Anttila 2000, 243.) Myös käänteinen nimipalvelu muodostaa puumallin. Kuviosta 7 selviää, miten osoitteen 195.47.37.2 käänteinen osoite muodostetaan. Käänteisen osoitteen muoto on tässä tapauksessa 2.37.47.195.in-addr.arpa. (Dostálek & Kabelová 2006, 8-9.)



KUVIO 7. Käänteisen nimipalvelun puumalli (Dostálek & Kabelová 2006, 9)

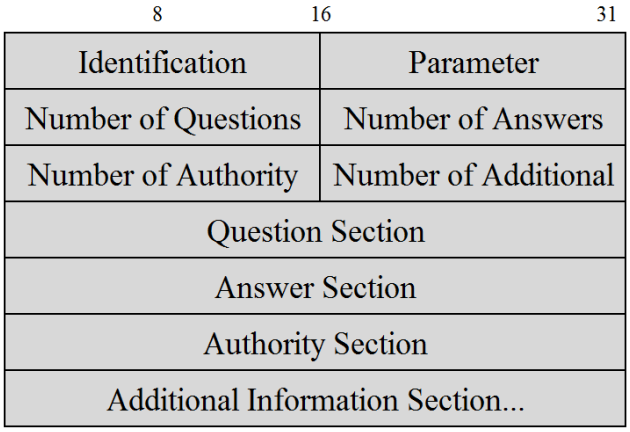
Kuvio 7 myös selvittää alustavasti käänteisen IPv6-osoitteen muodostumista. IPv6-osoitteet tulevat haaran ip6 alle. Myös IPv6-osoitteet esitetään käänteisessä järjestyksessä, mutta IPv6-osoitteen rakenteesta johtuen esitystapa on erilainen. Käänteisen IPv6-osoitteen muodostumista selittää seuraava esimerkki.

2001:708:410:3::1
2001:0708:0410:0003:0000:0000:0000:0001
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa

Käänteinen osoite IPv6-osoitteesta 2001:708:410:3::1 muodostuu yllä olevalla tavalla. Kaikki nolla-tavut on merkittävä käänteiseen osoitteeseen. (Britt ym. 2006, 430.)

DNS-kyselyt tehdään käyttäen UDP:tä. Nimipalvelukyselyt tulevat DNS-palvelimelle UDP-porttiin 53. DNS-kyselyiden ja -vastauksien muoto selviää kuviosta 8. Identification on numero, joka yksilöi kyselyn. Tämän avulla kysymys ja vastaus pystytään yhdistämään. Parameter määrittelee onko kysymyksessä kysely vai vastaus. Number of Questions ja Number of Answers -kentät pitävät

nimensä mukaisesti tiedon paketissa kulkevien kysymysten ja vastausten määrästä. Number of Authority -kenttä sisältää tiedon siitä, kuinka monta nimipalvelinta paketin Authority-osassa on listattu. Number of Additional -kenttä listaa paketin Additional Information -osassa olevien kenttien määrän. Question-osassa on DNS-kysely ja Answer-osassa vastaus. (Anttila 2000, 246-248.)



KUVIO 8. DNS-kyselyn ja vastauksen otsikkokentät (Anttila 2000, 246)

4.4 IPv4- ja IPv6-toteutusten erot

IPv4- ja IPv6-toteutustavat eroavat toisistaan siinä, minkä nimisiä tietueita zone-tiedostoissa on. Lisäksi DNS-palvelimen konfiguraatiossa pitää määrittää asetukset IPv6-osoitteiden kuuntelemiseksi. Tämän toteutustapa vaihtelee toteutusympäristöstä riippuen. Lisäksi asiakaskoneen, josta IPv6-nimikyselyjä suoritetaan, resolverin on pystyttävä käsittelemään IPv6:n tietuetyyppiä. Resolverin on osattava myös toimia tilanteessa, jossa nimikysely palauttaa IPv4- ja IPv6-osoitteen. Tällaisessä tilanteessa resolveri voi välittää nimikyselyn tehneelle ohjelmalle molemmat osoitteet tai vain toisen. Mikäli vain toinen osoite palautetaan, tapahtuu kommunikointi sen protokollan yli, esimerkiksi IPv4-osoitteella ohjelma käyttää IPv4-protokollaa. (Hagen 2006, 243-244.)

Kuviosta 9 selviää se, miten IPv4- ja IPv6-osoitteiden yhdistäminen verkkonimeen tapahtuu. Kuviossa IPv6-osoitteina on käytetty link-local-osoitteita, mutta tässä tapauksessa osoitetta voi ajatella miksi tahansa IPv6-osoitteeksi. A-

tietueella yhdistetään IPv4-osoite nimeen. AAAA-tietueella yhdistetään IPv6-osoite nimeen. (Hagen 2006, 243.)

```
$TTL 3h
$ORIGIN universe.com.
@       IN    SOA   ford.universe.com. mail.universe.com. (
        20011017    ; Serial
        3h          ; Refresh
        1h          ; Retry
        1w          ; Expire
        1h )        ; Minimum

universe.com.  IN NS  ford.universe.com.

ford  IN A  192.168.0.99
      IN AAAA fe80:0:0:0:2a0:24ff:fec5:3256
      IN A6 0 fe80:0:0:0:2a0:24ff:fec5:3256

arthur      IN A  192.168.0.66
      IN AAAA fe80:0:0:0:a00:20ff:fe20:adc2
      IN A6 0 fe80:0:0:0:a00:20ff:fe20:adc2

marvin      IN A  192.168.0.20
      IN AAAA fe80:0:0:0:202:b3ff:fe1e:8329
      IN A6 0 fe80:0:0:0:202:b3ff:fe1e:8329
```

KUVIO 9. Esimerkki IPv6-osoitteita sisältävästä zone-tiedostosta (Hagen 2006, 243)

Käänteinen zone-tiedosto sisältää muuten samat tiedot kuin zone-tiedosto, mutta nimi yhdistetään IPv4- tai IPv6-osoitteeseen käyttäen PTR-tietuetta. Lisäksi tiedoston $ORIGIN-toimialuemäärityksessä lukee toimialueen käänteinen nimi tai määritystä ei ole ollenkaan. Tämä riippuu siitä, missä muodossa PTR-tietueet halutaan kirjoittaa. Vaihtoehtoinen kirjoitustapa selvitetään käytännön osuuden käänteisten IPv6-tietueiden toteutuksen yhteydessä. Kuvio 10 esittää, miten käänteisessä zone-tiedostossa on yhdistetty nimi moon.universe.com PTR-tietueella IPv6-osoitteeseen 4321:0:1:2:3:4:567:89ab. (Hagen 2006, 242.)

```
b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA.IN
PTR   moon.universe.com
```

KUVIO 10. IPv6-osoitteen käänteinen nimitietue (Hagen 2006, 242)

5 DHCP JA IPv6

5.1 DHCP yleisesti

DHCP (Dynamic Host Configuration Protocol) on protokolla, jonka tehtävänä on automatisoida TCP/IP-verkossa olevien laitteiden konfiguroiminen. Protokollan avulla on mahdollista suorittaa samoja toimenpiteitä kuin verkon ylläpitäjä suorittaisi manuaalisesti verkkoon liittyvälle koneelle. Tällaisiä on esimerkiksi IP-osoitteen, aliverkon maskin, oletusyhdyskäytävän ja nimipalvelimien määrittäminen. DHCP vähentää myös virheiden mahdollisuutta, joita manuaalisesti asetusten määrittämisen yhteydessä voi tulla. (Droms & Lemon 2003, 3.)

5.2 Toiminta ja viestiliikenne

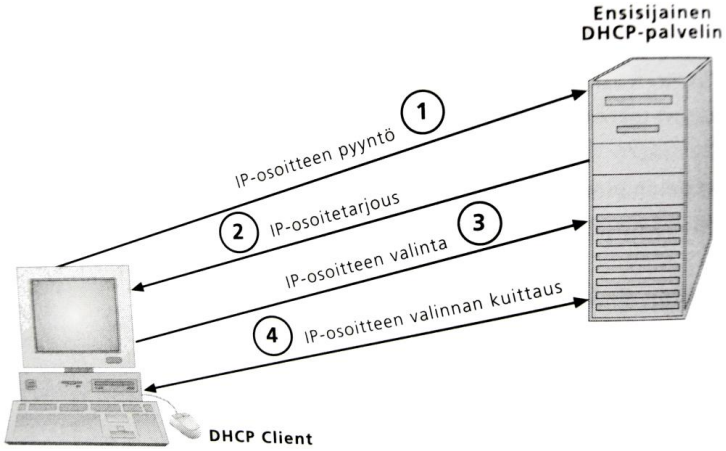
DHCP tukee kolmea eri mekanismia IP-osoitteiden määrittelyyn, jotka ovat

- automaattinen määrittely,
- dynaaminen määrittely ja
- määrittely käsin.

Automaattisessa määrittelyssä DHCP-palvelin antaa osoitteen osoitetta pyytävälle laitteelle määrittelemättömäksi ajaksi. Dynaamisessa määrittelyssä osoitteen käyttöaika on määritelty. Käsin määrittelyssä DHCP-palvelimeen määritellään laitteelle IP-osoite esimerkiksi laitteen MAC-osoitteen perusteella. Näin ollen laite, jonka MAC-osoitteelle on määritelty tietty IP-osoite, saa kyseisen osoitteen liittyessään verkkoon. Näistä kolmesta mekanismista käytetyin on dynaaminen määrittely, koska se mahdollistaa sen, että IP-osoitteita ei käytetä turhaan. IP-osoitteet palautuvat takaisin jaettaviksi vuokra-ajan umpeutumisen jälkeen. (Anttila 2000, 203.)

Kuviosta 11 selviää esimerkki IPv4:n DHCP-palvelimen toiminnan periaatteesta. Tapahtumaketju alkaa siitä, kun työasema, jonka verkkoasetuksissa on määritelty IP-osoitteen määrittäminen käyttäen DHCP-palvelua, liittyy verkkoon. Tapahtumaketjun aikana työasema ja palvelin vaihtavat keskenään DHCP-

sanomia, joita ovat DHCPDISCOVER (1), DHCPOFFER (2), DHCPREQUEST (3) ja DHCPACK (4). Taulukko 3 listaa DHCP- ja DHCPv6-sanomat ja kuvaa ne.



KUVIO 11. DHCP-sanomat palvelimen ja työaseman välillä (Anttila 2000, 208)

TAULUKKO 3. DHCP- ja DHCPv6-sanomien tyypit (Davies 2012, 213)

Msg-Type	Message	Description	Equivalent DHCP for IPv4 Message
1	Solicit	Sent by a client to locate servers.	DHCPDiscover
2	Advertise	Sent by a server in response to a Solicit message to indicate availability.	DHCPOffer
3	Request	Sent by a client to request addresses or configuration settings from a specific server.	DHCPRequest
4	Confirm	Sent by a client to all servers to determine whether a client's configuration is valid for the connected link.	DHCPRequest
5	Renew	Sent by a client to a specific server to extend the lifetimes of assigned addresses and obtain updated configuration settings.	DHCPRequest
6	Rebind	Sent by a client to any server when a response to the Renew message is not received.	DHCPRequest
7	Reply	Sent by a server to a specific client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.	DHCPAck
8	Release	Sent by a client to indicate that the client is no longer using an assigned address.	DHCPRelease
9	Decline	Sent by a client to a specific server to indicate that the assigned address is already in use.	DHCPDecline
10	Reconfigure	Sent by a server to a client to indicate that the server has new or updated configuration settings. The client then sends either a Renew or an Information-Request message.	N/A
11	Information-Request	Sent by a client to request configuration settings (but not addresses).	DHCPInform
12	Relay-Forward	Sent by a relay agent to forward a message to a server. The Relay-Forward contains a client message encapsulated as the DHCPv6 Relay-Message option.	N/A
13	Relay-Reply	Sent by a server to send a message to a client through a relay agent. The Relay-Reply contains a server message encapsulated as the DHCPv6 Relay-Message option.	N/A

5.3 DHCP-vikasietoisuus

DHCP-palvelimen vikasietoisuus on toteutettavissa sillä, että verkossa on käytössä useampia DHCP-palvelimia. Nämä palvelimet voivat toimia joko toisistaan tietämättöminä tai niin, että niiden toiminta sisältää keskenään viestimistä. Ensimmäisessä tapauksessa toissijainen DHCP-palvelin voidaan määrittää jakamaan eri osoitealuetta. Toisessa tapauksessa ratkaisu on failover-protokollan käyttäminen. (Droms & Lemon 2003, 295.)

DHCP failover -protokollan avulla on mahdollista toteuttaa vikasietoisuus, jossa ensisijainen ja toissijainen palvelin jakavat osoitteita samasta osoiteavaruudesta. Failover-protokollalla toteutettu vikasietoisuus kuitenkin vaatii sen, että DHCP-palvelimilla on käytössä jonkinlainen tietokanta IP-osoitteista. (Droms & Lemon 2003, 159.)

5.4 IPv4- ja IPv6-toteutusten erot

DHCP ja DHCPv6 käyttävät molemmat UDP-protokollaa sanomien välityksessä. DHCP:ssä työasema käyttää UDP-porttia 68 ja palvelin UDP-porttia 67. DHCPv6:ssa työasemassa käytetään UDP-porttia 546 ja palvelimessa UDP-porttia 547. (Anttila 2000, 203; Davies 2012, 212.)

Tilaton autokonfiguraatio on IPv6:n tuoma uudistus. Tilattomassa autokonfiguraatiossa verkon reititin lähettää verkon laitteille tiedon siitä, mitkä 64 bittiä ovat verkon prefix. Laite muodostaa tämän jälkeen IPv6-osoitteen loppuosan laitteen verkkoliitännän MAC-osoitteesta. Mikäli verkossa on useampia reitittimiä, jotka mainostavat eri prefixiä, muodostaa laite useampia IPv6-osoitteita samalla tavalla. Tilattoman autokonfiguraation etu on siinä, että verkkoon liittyvät laitteet eivät tarvitse minkäänlaista manuaalista konfiguroimista. (van Beijnum 2006, 3.)

6 KÄYTÄNNÖN TOTEUTUS

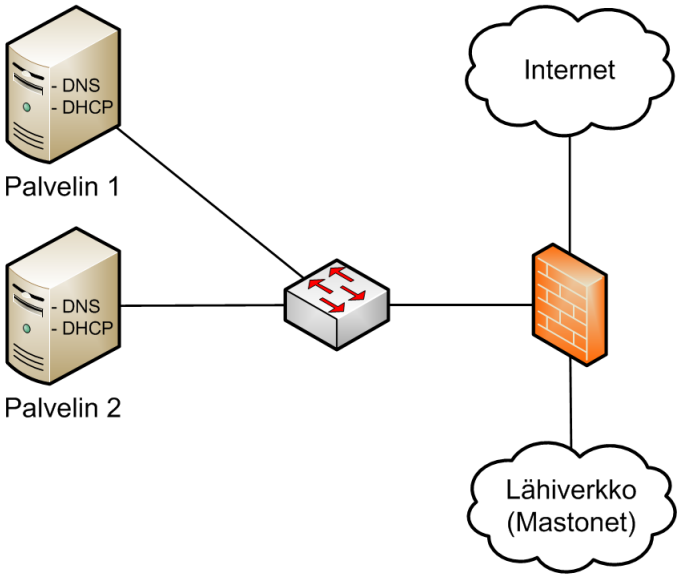
6.1 Testiympäristön kuvaus

Opinnäytetyön käytännön osuudessa toteutettiin testiympäristö, jossa testattiin DHCP:n ja DNS:n toimintaa IPv6:n kanssa. Toteutus liittyi Lahden ilmaisen langattoman verkon, Mastonetin, kehittämiseen. Testiympäristön pohjana oli Mika Pesosen opinnäytetyössään "Virtualisoidut verkkopalvelut" suunnittelemat ja toteuttamat Mastonetin verkkopalvelut. Pesosen työssä ympäristö toteutettiin IPv4-yhteensopivana. (Pesonen 2010.) Tässä opinnäytetyössä toteutettiin samankaltainen ympäristö kuin Pesosen suunnittelema Mastonetin nykyinen ympäristö ja jatkettiin sitä IPv6-yhteensopivaksi. Tässä työssä ei keskitytty määrittämään kaikkia palvelinkäytössä hyödyllisiä ominaisuuksia palvelimiin, vaan työn painopiste oli IPv6-ominaisuuksien käyttöönotossa. Testiympäristö toteutettiin Mastonetin nykyisen ympäristön mukaisten CentOS-palvelimien lisäksi myös Windows-palvelimilla. CentOS-palvelinten toteutus IPv4:n osalta on toteutettu Pesosen työn dokumentoinnin mukaisesti.

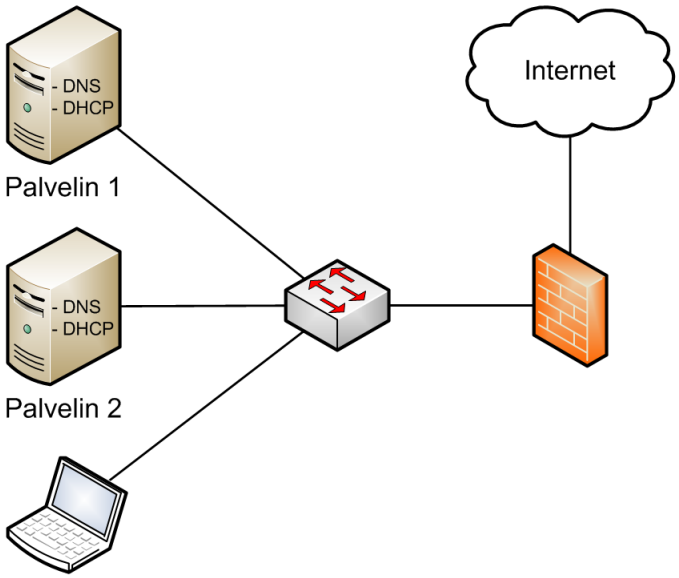
Opinnäytetyön käytännön osuuden testiympäristö koostui palvelintietokoneesta, johon oli asennettu VMware ESXi 5.0 -palvelinohjelmisto. Palvelintietokone oli Intel® Core™2 Quad CPU Q6600 @ 2.40 GHz ja siinä oli 8 GB muistia. ESXi-palvelimen virtualisointiympäristöön asennettiin virtuaalikoneita palvelimen hallintaan tarkoitetulla VMware vSphere Client -ohjelman avulla, jotka muodostivat testiympäristön. Testiympäristö muodostui kuudesta eri virtuaalikoneesta. Neljä koneista oli palvelimia, joissa kahdessa oli käyttöjärjestelmänä Windows Server 2008 R2 ja kahdessa CentOS 6.2. Palvelinkoneiden lisäksi käytössä oli palomuuri, joka oli FreeBSD Unix-käyttöjärjestelmään pohjautuva pfSense 2.0.1. Lisäksi ympäristöön kuului yksi testikone, jonka käyttöjärjestelmä oli Windows 7.

Testiympäristön toteutuksen tapahtuessa virtuaaliympäristössä käytettiin järjestelmän luomisessa virtuaalikytkintä. Virtuaalikytkimen ansiosta oli mahdollista toteuttaa verkon toiminta suunnitellusti. Toteutuksen pohjana oli ensin kuviosta 12 selviävä verkkokuva. Verkon rakenne kuitenkin muuttui toteutuksen aikana kuvion 13 mukaiseksi. Ensimmäisen suunnitelman mukainen

verkon rakenne olisi vastannut Mastonet-verkon oikeaa rakennetta. Verkon rakenteen muuttamisen syy oli testien yksinkertaistaminen. Kuitenkin alkuperäistä verkon rakennetta, jossa testikone sijaitsi LAN-verkossa, käytettiin työn aluksi IPv4-testauksissa. IPv6-testauksien aikana testikone muutettiin samaan verkkoon palvelimien kanssa. Verkko, jossa palvelimet sijaitsivat oli DMZ (demilitarized zone, demilitarisoitu alue) eli aliverkko, josta yhteys Internetiin meni palomuurin kautta.



KUVIO 12. Suunnitellun testiympäristön verkkokuva



KUVIO 13. Toteutuneen testiympäristön verkkokuva

Testiverkossa käytettiin IPv4- ja IPv6-osoitteita. Osoitealueet oli määritetty testitarkoitukseen. Todellisessa toteutuksessa osoitealueiden laajuutta olisi hyvä suunnitella tarkemmin käyttötarkoituksen mukaan. Testiverkossa käytetyt IPv4- ja IPv6-osoitteet ja -osoitealueet selviävät taulukosta 4.

TAULUKKO 4. Työssä käytetyt IPv4- ja IPv6-osoitteet ja -osoitealueet

Verkko / Laite	**IPv4- ja IPv6-osoitteet ja -osoitealueet**
LAN-verkko	192.168.1.0/24
LAN-verkon gateway	192.168.1.1
DMZ-verkko	172.31.31.0/24 2001:708:410:3::/64
DMZ-verkon gatewayt	172.31.31.254 2001:708:410:3::1
winserver1	172.31.31.10 2001:708:410:3::10
winserver2	172.31.31.20 2001:708:410:3::20
centos1	172.31.31.30 2001:708:410:3::30
centos2	172.31.31.40 2001:708:410:3::40

6.2 Virtualisointiympäristö

6.2.1 Virtuaalikoneiden asentaminen

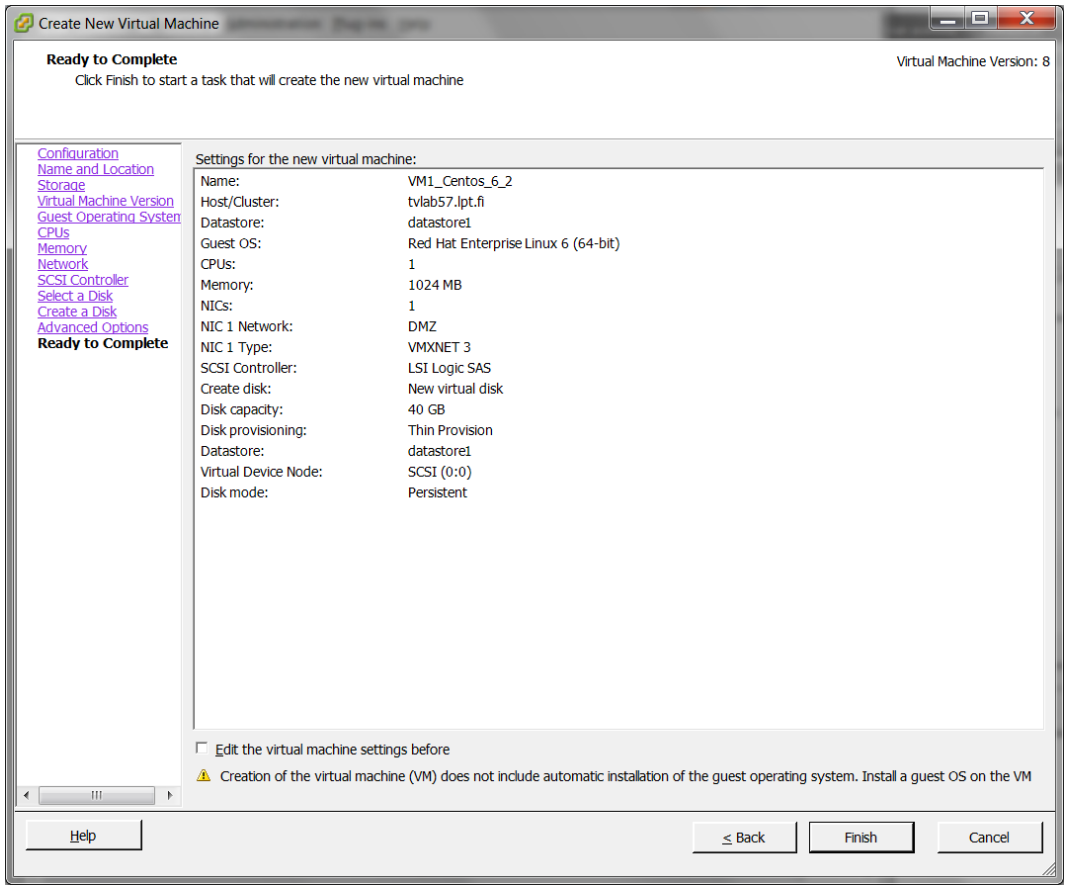
VMware ESXi 5.0 -palvelimen virtualisointiympäristöä käytettiin VMware vSphere Client -ohjelman avulla. Ohjelman suora latauslinkki löytyi ottamalla yhteys palvelimeen www-selaimella. Ohjelma asennettiin sivun latauslinkistä palvelimen hallintaan tarkoitetulle koneelle oletusasetuksin. Ohjelman asentamisen jälkeen ohjelman avulla kirjauduttiin palvelimeen palvelimen käyttäjätunnuksella ja salasanalla.

VMware vSphere Client -ohjelmassa virtuaaliympäristöä päästiin hallinnoimaan valitsemalla aloitusruudusta Inventory. Uusien virtuaalikoneiden luominen tapahtui Getting Started -välilehdellä valitsemalla "Create a new virtual machine". Jokaista virtuaalikonetta luodessa määriteltiin koneen kokoonpanoksi mukautettu. Virtuaalikoneet luotiin seuraavilla asetuksilla.

- Asennustavaksi (Configuration) valittiin Custom.
- Koneen nimi (Name and Location) määritettiin asennettavan koneen mukaan, esim. VM1_Centos_6_2.
- Tiedon tallennuspaikaksi (Storage) valittiin datastore1.
- Virtuaalikoneen versioksi (Virtual Machine Version) valittiin 8.
- Koneen käyttöjärjestelmä (Guest Operating System) määritettiin asennettavan koneen mukaan, esim. Red Hat Enterprise Linux 6 (64-bit).
- Suoritinmäärityksissä (CPUs) valittiin suorittimien määräksi 1.
- Muistin määräksi (Memory) valittiin 1 GB.
- Käytettäväksi verkkosovittimeksi (Network) valittiin DMZ. Mikäli DMZ-verkkoa ei oltu asennusvaiheessa vielä luotu (kts. luku 6.2.2), valittiin tähän verkkokortti mitä haluttiin käytettävän.
- Tietoliikenneväyläasetuksiksi (SCSI Controller) valittiin LSI Logic SAS.
- Valittiin virtuaalilevyn valinnassa (Select a Disk) "create a new virtual disk".
- Virtuaalilevyn luomisessa (Create a Disk) levyn kooksi valittiin 40 GB, levyn provisioinniksi "Thin Provision" ja sijainniksi valittiin "Store with the virtual machine".

- Lisäasetuksia (Advanced Options) ei määritetty.

Kuvio 14 esittää virtuaalikoneen asetukset valmiina virtuaalikoneen luomista varten. Luontivelhon ikkunan alalaidassa näkyy huomautus siitä, että virtuaalikoneen luominen ei sisällytä käyttöjärjestelmän asennusta virtuaalikoneeseen. Tämä pitää tehdä jokaisen virtuaalikoneen kohdalla erikseen.



KUVIO 14. Virtuaalikoneen asetukset määriteltyinä

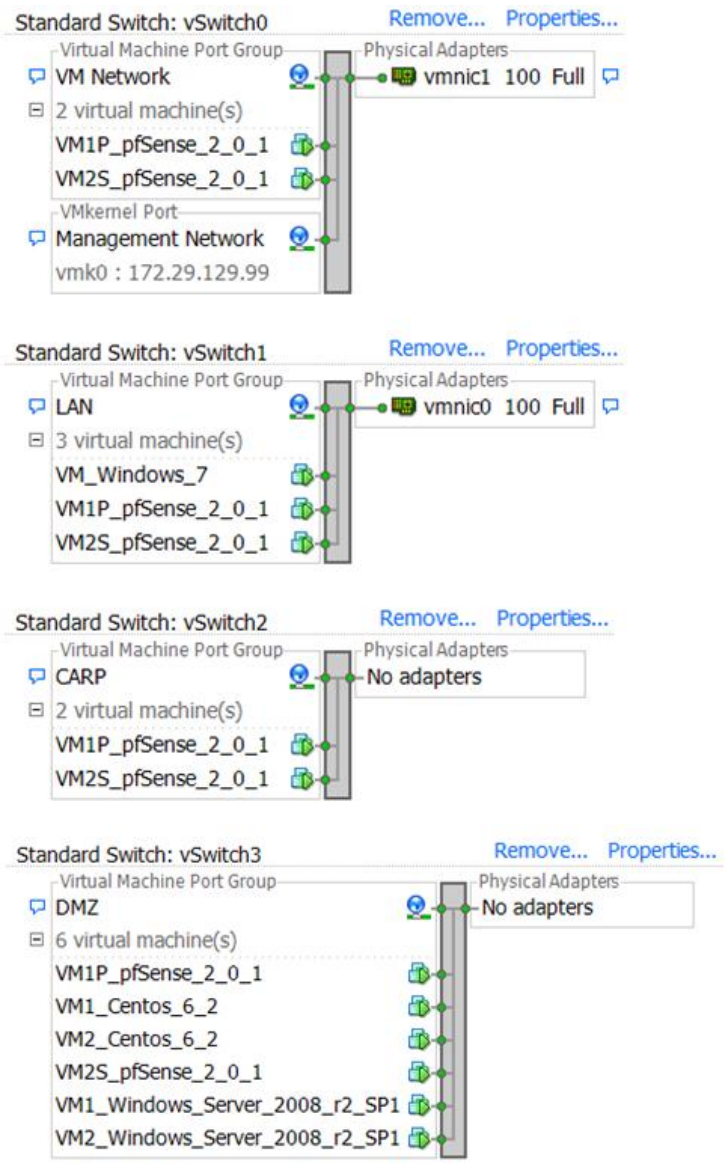
Virtuaalikoneen luomisen jälkeen luodun virtuaalikoneen asetuksia muokattiin valitsemalla virtuaalikoneen Getting Started -välilehdeltä "Edit virtual machine settings". Asetuksissa muokattiin asennusmedia virtuaalikoneen CD/DVD-aseman käyttöön. Tämä tehtiin muokkaamalla CD/DVD-aseman device type -valinnaksi "Datastore ISO File" ja tämän jälkeen Browse-valinnalla haettiin datastore1:stä tarvittava asennusmedia. Asennusmedia oli tätä ennen lisätty datastoreen vSphere

Clientin Summary-välilehdellä valitsemalla hiiren oikealla painikkeella Storage-ikkunassa näkyvän datastore1:n päällä ”Browse Datastore...”. Valinnalla avautuvassa Datastore Browserissa asennusmedian, ISO-tiedoston, lataaminen tapahtui Upload files to this datastore -valinnalla.

Virtuaalikoneen asetuksista valittiin vielä Options-välilehdeltä Advanced-asetuksien alta löytyvästä Boot Options -asetuksista valinta ”The next time the virtual machine boots, force entry into the BIOS setup screen.” aktiiviseksi. Tällä asetuksella virtuaalikone pakotettiin BIOS-asetuksiin seuraavan käynnistyksen yhteydessä. Tämän jälkeen virtuaalikone oli valmis asennettavaksi. Virtuaalikone käynnistettiin Power On -painikkeesta ja virtuaalikoneen konsolinäkymän sai avattua painamalla virtuaalikoneen päällä hiiren oikeaa painiketta ja valitsemalla ”Open Console”. Tämän jälkeen BIOS-asetuksiin päästiin muuttamaan boot-asetuksista ensisijaiseksi CD/DVD-asema, jonka jälkeen asennusmedian asentaminen onnistui virtuaalikoneeseen yhdistetystä ISO-tiedostosta.

6.2.2 Virtuaalikytkimen määritykset

Testiverkon toteutuksessa käytettiin virtuaalikytkimiä. Virtuaalikytkimen määritykset selviävät kuviosta 15. Kuviosta selviää se, missä verkoissa toteutuksen palvelimet ja testikone sijaitsivat. Palvelimet sijaitsivat DMZ-verkossa ja testikone LAN-verkossa. Myöhemmin IPv6-testauksien aikana testikone muutettiin samaan verkkoon kuin palvelimet. Kuviossa näkyy myös miten pfSense-palomuuri oli määritelty verkkoon.



KUVIO 15. Virtuaalikytkimen määritykset

6.3 Windows Server 2008 R2 -palvelimet

6.3.1 Palvelimien asennus ja verkkoasetukset

Windows Server 2008 R2 -palvelimien asennuksissa käytettiin 64-bittistä versiota, jossa Service Pack 1 oli valmiiksi asennettuna. Ensimmäiselle palvelimelle annettiin nimeksi winserver1 ja toiselle winserver2. Asennuksen jälkeen palvelimiin asennettiin kaikki saatavilla olevat päivitykset. IP-osoitteeksi winserver1-palvelimeen määritettiin 172.31.31.10 ja winserver2-palvelimeen 172.31.31.20. Aliverkon peitteenä käytettiin 255.255.255.0.

Oletusyhdyskäytäväksi määritettiin 172.31.31.254, joka fyysisesti oli pfSense-palomuurin DMZ-verkon osoite. Verkkoasetuksissa ensisijaisen DNS-palvelimen osoitteeksi määritettiin 172.31.31.10 eli winserver1:n osoite ja vaihtoehtoisen DNS-palvelimen osoitteeksi lisättiin 172.31.31.20 eli winserver2:n osoite. Winserver2-palvelimessa DNS-osoitemääritykset laitettiin toisin päin eli ensisijaiseksi DNS-palvelimeksi määritettiin winserver2:n osoite ja vaihtoehtoiseksi winserver1:n osoite. IPv6-osoite winserver1:llä oli 2001:708:410:3::10/64 ja winserver2:lla 2001:708:410:3::20/64, jotka vastaavasti määritettiin samalla tyylillä DNS-palvelimien osoitteiksi kuin IPv4-osoitemäärityksissä.

6.3.2 DNS- ja DHCP-palvelimien asennus

DNS:n ja DHCP:n asentaminen toimimaan IPv4:n kanssa alkoi roolien lisäämisellä ensimmäiseen palvelimeen. Tämä tapahtui Initial Configuration Tasks -ikkunassa valitsemalla Customize This Server -työkalujen alta ”Add roles”. Roolien lisääminen tapahtui asennusvelhon avustuksella, jossa tehtiin seuraavat määritykset.

- Valittiin ”Next” aloitusikkunassa.
- Valittiin asennettavaksi ”DHCP Server” ja ”DNS Server”.
- Valittiin ”Next” DNS-palvelimesta tietoa antavassa ruudussa.
- Valittiin ”Next” DHCP-palvelimesta tietoa antavassa ruudussa.
- Valittiin palvelimen IP-osoite toimimaan DHCP-palvelimena.
- Määritettiin palvelimen toimialueeksi inside.lpt.fi ja ensisijaisen DNS-palvelimen IP-osoitteeksi 172.31.31.10. Toissijaisen DNS-palvelimen osoitteeksi määritettiin 172.31.31.20.
- WINS-asetuksia ei muutettu.
- Lisättiin DHCP scope eli jaettava osoitealue valitsemalla ”Add...”.
- Osoitealueen nimeksi määritettiin ”inside-network”, osoitealueen ensimmäiseksi osoitteeksi 192.168.1.10, viimeiseksi osoitteeksi 192.168.1.254 ja aliverkon tyypiksi valittiin ”Wireless”. Valittiin ”Activate this scope”. Aliverkon peitteeksi määritettiin 255.255.255.0 ja oletusyhdyskäytäväksi 192.168.1.1.
- Jatkettiin asennusta valitsemalla ”Next”.

- Poistettiin tilaton autokonfiguraatio käytöstä valitsemalla ”Disable DHCPv6 stateless mode for this server”.
- Valittiin asennuksen vahvistusikkunassa ”Install”.
- Suljettiin asennusikkuna valitsemalla ”Close”.

DNS asennettiin loppuun avaamalla palvelimessa DNS Manager ja määrittämällä forward ja reverse lookup zonet ”Configure a DNS Server...” -asennusvelhossa. Tämä tapahtui seuraavilla määrityksillä.

- Valittiin ”Next” aloitusikkunassa.
- Valittiin ”Create forward and reverse lookup zones (recommended for large networks)”.
- Valittiin tyypiksi ”Primary zone”.
- Alueen nimeksi määritettiin ”inside.lpt.fi”.
- Luotiin uusi zone-tiedosto nimellä ”inside.lpt.fi.dns”.
- Ei otettu käyttöön dynaamisia päivityksiä valinnalla ”Do not allow dynamic updates”.
- Luotiin reverse lookup zone valitsemalla ”Yes, create a reverse lookup zone now”.
- Valittiin tyypiksi ”Primary zone”.
- Valittiin luotavaksi ”IPv4 Reverse Lookup Zone”.
- Määritettiin verkon ID:ksi ”172.31.31”.
- Luotiin uusi zone-tiedosto nimellä ”31.31.172.in-addr.arpa.dns”.
- Ei otettu käyttöön dynaamisia päivityksiä.
- Ei valittu DNS-kyselyiden eteenpäin välittämistä valinnalla ”No, it should not forward queries”.
- Viimeisteltiin asennus valitsemalla ”Finish”.

Tämän jälkeen määritettiin samalla tavalla reverse lookup zone IPv4-verkolle 192.168.1.0/24 ja IPv6-verkolle 2001:708:410:3::/64. Reverse lookup zonea IPv6-verkolle määritellessä valittiin asennusvelhossa luotavaksi "IPv6 Reverse Lookup Zone".

DNS-palvelimeen lisättiin A-tietueita forward lookup zoneen. Tämä tapahtui painamalla hiiren oikeaa painiketta inside.lpt.fi-toimialueen päällä ja valitsemalla ”New Host (A or AAAA)...”. Testiympäristössä määritettiin A-tietue

winserver1:lle (172.31.31.10) ja winserver2:lle (172.31.31.20). AAAA-tietueet IPv6-osoitteille lisättiin winserver1:lle ja winserver2:lle samalla valinnalla kuin A-tietueet oli lisätty, mutta IPv4-osoitteen sijasta osoitekenttään kirjoitettiin IPv6-osoite. A- tai AAAA-tietueita lisättäessä valinta "Create associated pointer (PTR) record" loi samalla käänteisen nimitietueen reverse lookup zonen alle.

Toissijaisen DNS-palvelimen käyttöönotto (winserver2) vaati ensin muutoksen winserver1-palvelimeen. Tämä tehtiin inside.lpt.fi-toimialueen asetuksiin valitsemalla Zone Transfers -välilehdeltä ”Allow zone transfers” ja ”Only to servers listed on the Name Servers tab”. Tämän jälkeen toissijainen DNS-palvelin eli winserver2 lisättiin ”Name Servers”-välilehdellä nimipalvelimien listaan. Listaan tuli näkymään winserver2:n IPv4- ja IPv6-osoitteet. Tämän jälkeen winserver2-palvelimeen asennettiin DNS-palvelinrooli, jonka jälkeen palvelimeen lisättiin forward lookup zone New Zone Wizard -asennusvelhon avulla. Asennuksessa valittiin lisättäväksi secondary zone -alueeksi inside.lpt.fi. Secondary zone -aluetta lisättäessä asennusvelho kysyi DNS-palvelinta, josta alue kopioidaan. Sellaiseksi lisättiin winserver1. Tässäkin kohdassa näkyviin tuli palvelimen IPv4- ja IPv6-osoitteet. Lopuksi lisättiin reverse lookup zonet jokaiselle verkolle secondary zone -valinnalla. Jokaisen verkon kohdalla lisättiin winserver1 zone-tiedostojen kopioimisen lähteeksi. Winserver1-palvelimessa piti lopuksi tarkistaa se, että jokaisen reverse lookup zonen asetuksissa oli Zone Transfers -välilehdellä valittuna ”Allow zone transfers” ja ”Only to servers listed on the Name Servers tab”. Lisäksi Name Servers -välilehdeltä piti löytyä winserver2 (IPv4- ja IPv6-osoitteet).

DHCP:n konfiguroiminen jakamaan IPv6-osoitteita tapahtui DHCP-palvelimen asetuksissa winserver1-palvelimella. IPv6:n alle lisättiin uusi osoitealue (new scope) asetusvelhon avulla, jossa määritettiin verkoksi 2001:708:410:3::/64. Osoitealueesta määritettiin jätettäväksi pois osoitteiden jaosta alue 2001:708:410:3::1 – 2001:708:410:3::40. Lopuksi määritettiin osoitteiden eliniät (preferred ja valid) ja aktivoitiin osoitealue. IPv6-osoitealueen asetuksia päästiin määrittämään ”Scope Options” -kohdassa valinnalla ”Configure Options...”. Kohtaan ”DNS Recursive Name Server IPv6 Address List” määritettiin DNS-palvelimien IPv6-osoitteet (2001:708:410:3::10 ja 2001:708:410:3::20). Kohtaan ”Domain Search List” määritettiin inside.lpt.fi.

DHCP-palvelimen IPv6-asetuksien määrittämisen lisäksi piti osoitteiden jakamisen toimimiseksi antaa palvelimen komentokehotteessa komennot ”netsh int ipv6 set int [verkkoliitännän numero] managedaddress=enabled” ja ”netsh int ipv6 set int [liitännän numero] otherstateful=enabled”. Käytössä olevan verkkoliitännän numeron pystyi selvittämään komennolla ”netsh int ipv6 show int”. Tämän lisäksi palvelimeen piti määrittää reitti, jonka palvelin jakoi asiakaskoneille. Ilman tätä määritystä testiympäristössä ei testikone pystynyt pingaamaan palvelinta. Reitti määritettiin komennolla ”netsh interface ipv6 add route 2001:708:410:3::/64 [liitännän numero] publish=yes”.

Vikasietoinen DHCP IPv4:n osalta toteutettiin Windows Server 2008 R2 -palvelimissa valmiiksi olevalla split-scope-ominaisuudella. Ensin winserver2-palvelimeen asennettiin DHCP-palvelinrooli samoin asetuksin kuin winserver1-palvelimeen oli asennettu aiemmin. Asennuksessa ei kuitenkaan määritetty mitään jaettavaa osoitealuetta. Tämän jälkeen winserver1-palvelimella painettiin tietyn IPv4-osoitealueen päällä hiiren oikeaa painiketta ja valittiin Advanced-valinnan alta ”Split-Scope”. Valinnalla avautuvassa asetusvelhossa määritettiin toiseksi DHCP-palvelimeksi winserver2. Tämän jälkeen määritettiin kuinka suuri osoitealueen jako kahden palvelimen välille muodostetaan. Testiverkossa valittiin winserver1:n käyttöön 80 prosenttia osoitteista ja winserver2:n käyttöön 20 prosenttia. Viimeiseksi asetusvelhossa oli mahdollista määrittää viive millisekunneissa milloin toinen DHCP-palvelin alkaa jakamaan osoitteita. Split-scope-ominaisuus toteutettiin muille IPv4-osoitealueille samalla tavalla. IPv6-osoitealueelle split-scope-ominaisuus ei ollut käytettävissä. Korvaava vaihtoehto split-scope-ominaisuuden käyttämiselle on IPv6:n osalta laittaa toinen palvelin jakamaan eri osoitealuetta kuin ensisijainen palvelin jakaa.

6.4 CentOS 6.2 -palvelimet

6.4.1 Palvelimien asennus ja verkkoasetukset

CentOS 6.2 -palvelimet asennettiin minimiasennuksella. Tämä tarkoittaa sitä, että asennusvaiheessa valittiin asetukset, joilla palvelimiin asentui mahdollisimman vähän paketteja. Ylimääräisten palveluiden ja ohjelmien pois jättäminen auttaa

palvelimen suorituskykyyn ja parantaa myös tietoturvaa. Asennuksen jälkeen palvelimiin asennettiin päivitykset ja muita palvelinkäytössä hyödyllisiä ominaisuuksia. Palvelimen asennus tapahtui seuraavin asetuksin.

- Valittiin "Install or upgrade an existing system".
- Valittiin "Skip" asennusmedian testaamisen kysymykseen. Tarvittaessa asennusmedian pystyi testaamaan valitsemalla "OK".
- Asennuksen aloitusruudusta edettiin valitsemalla "Next".
- Asennuskieleksi valittiin "English (English)".
- Käytettäväksi näppäimistöasetteluksi valittiin "Finnish (latin1)".
- Valittiin käytössä oleviksi laitteiksi "Basic Storage Devices".
- Levyn alustuksessa valittiin "Apply my choice to all devices with undetected partitions or filesystems" ja valittiin "Yes, discard any data".
- Määritettiin palvelimen nimi, esim. centos1.inside.lpt.fi.
- Aikavyöhykkeeksi valittiin "Europe/Helsinki". "System clock uses UTC" -valinta jätettiin päälle.
- Määritettiin root-käyttäjätunnuksen salasana.
- Asennustyypiksi valittiin "Use All Space". Asetukset "Encrypt system" ja "Review and modify partitioning layout" jätettiin valitsematta.
- Kirjoitettiin asetukset levylle valitsemalla "Write changes to disk".
- Valittiin asennusmuodoksi "Minimal" ja valittiin "Customize now" asennettavien ohjelmien muokkaamiseksi.
- Poistettiin kaikista asennuspaketeista valinnat.
- Kun asennus oli valmis käynnistettiin kone valitsemalla "Reboot".

Asennuksen jälkeen palvelimiin asennettiin päivitykset komennolla "yum -y update". Päivityksien lisäksi asennettiin nano-tekstieditori kirjoittamalla komento "yum install nano". Komennolla "yum install irqbalance" saatiin tuki useammalle prosessorille. Ylimääräiset palvelut netfs, lvm2-monitor ja postfix poistettiin käytöstä komennolla ”chkconfig [palvelu] off”. Yum-päivitykset saadaan päivittymään automaattisesti kerran päivässä seuraavilla kommennoilla.

```
chkconfig crond on
chkconfig yum-cron on
service yum-cron start
```

Päällä olevat palvelut pystyi tarkistamaan komennolla ”chkconfig --list | grep ”3:on” ”.

Seuraavaksi otettiin pois käytöstä SELinux muokkaamalla palvelun konfiguraatiotiedostoa nano-tekstieditorilla komennolla ”nano /etc/selinux/config” ja määrittämällä tiedostoon asetus ”SELINUX=disabled”. Mikäli SELinux jätetään päälle, saattaa se estää DNS-palvelinten vikasietoisuuden toiminnan. CentOS-palvelimen SSH-asetuksien konfiguroiminen tapahtuu muokkaamalla tiedostoa ”/etc/ssh/sshd_config”. Testiympäristössä SSH-asetuksia ei muokattu, mutta normaalissa palvelinkäytössä nämä asetukset on hyvä tarkistaa käyttötarkoituksen mukaiseksi. Palvelimiin ladattiin vielä NTP-palvelu komennolla ”yum install ntp”. Palvelu otettiin käyttöön komennolla ”chkconfig ntpd on”. Synkronointiasetuksiksi määritettiin ”ntpdate pool.ntp.org”. Lopuksi käynnistettiin palvelu komennolla ”/etc/init.d/ntpd start”. NTP-palvelu synkronoi ajan aikapalvelimilta. Palvelimien ajan synkronoiminen on tärkeää, koska palvelimille asennetaan palveluita, joista tehdään vikasietoiset. Tämän vuoksi on tärkeää, että palvelimien ajat ovat samat.

Palvelimien verkkoliitännän asetukset määritettiin seuraavanlaisiksi tiedostoon ”/etc/sysconfig/network-scripts/ifcfg-eth0”, jossa eth0 oli käytössä oleva verkkoliitäntä.

```
DEVICE=”eth0”
BOOTPROTO=static
HWADDR=”xx:xx:xx:xx:xx:xx”
IPADDR=172.31.31.30                (centos2: 172.31.31.40)
BROADCAST=172.31.31.255
NETMASK=255.255.255.0
NETWORK=172.31.31.0
IPV6INIT=yes
IPV6ADDR=2001:708:410:3::30      (centos2: 2001:708:410:3::40)
IPV6_DEFAULTGV=2001:708:410:3::1
ONBOOT=yes
```

Verkkoliitännän asetuksien määrityksen jälkeen uusien asetuksien käyttöönotto tapahtui komennoilla ”ifdown eth0” ja ”ifup eth0”.

Verkkoasetukset määriteltiin tiedostoon ”/etc/sysconfig/network” seuraaviksi.

```
NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=centos1                (centos2: centos2)
GATEWAY=”172.31.31.254”
```

Nimipalvelimien määrittäminen tapahtui tiedostossa ”/etc/resolv.conf”. Ensisijaiseksi nimipalvelimeksi määritettiin centos1-palvelimessa palvelimen oma osoite ja toissijaiseksi centos2:n osoite. Määritykset tehtiin centos2-palvelimeen toisin päin eli ensisijaiseksi nimipalvelimeksi tuli centos2:n osoite ja toissijaiseksi centos1:n osoite. Centos1-palvelimen resolv.conf-tiedoston määritykset olivat seuraavanlaiset.

```
domain inside.lpt.fi
nameserver 172.31.31.30
nameserver 172.31.31.40
nameserver 2001:708:410:3::30
nameserver 2001:708:410:3::40
```

Ennen kuin CentOS-palvelimien nimipalvelut olivat toiminnassa, käytettiin asennuksien aikana toimivaa nimipalvelinta. Tällaisia oli esimerkiksi aikaisemmin konfiguroidut winserver1 (172.31.31.10) ja winserver2 (172.31.31.20). DHCP-palvelimen osalta CentOS-palvelinten testivaiheessa otettiin Windows-palvelimilta DHCP-palvelu pois päältä. Näin ollen oli varmaa se, että testikone yritti hakea IPv4- ja IPv6-osoitteet testattavilta palvelimilta. Kun Windows-palvelinten DNS-palvelimia ei enää tarvittu, Windows-palvelimet oli mahdollista sammuttaa virtuaalikoneiden hallinnasta.

Tarvittavien palveluiden ja verkkoasetuksien määrittämisen jälkeen siirryttiin asennuksessa toteuttamaan Mastonetin nykyinen ympäristö ja lisäämään ympäristöön IPv6-ominaisuudet. Alkuperäisessä dokumentaatiossa on kuvattu palomuurisäännöt, DHCP-palvelimen asentaminen vikasietoisena (IPv4) ja DNS-palvelimen asentaminen vikasietoisena (IPv4). Koska IPv4-ympäristö on aiemmin suunniteltu, ei IPv4-konfigurointeja kuvata yksityiskohtaisesti. Tarkemmin kuvataan ne muutokset, mitä vaaditaan ympäristön saamiseksi toimintaan IPv6:n kanssa. Kaikki oleelliset konfiguraatiot löytyvät työn liitteistä.

6.4.2 Palomuurisäännöt

Palomuurisääntöjen määrittäminen palvelimiin tapahtui muokkaamalla tiedostoa ”/etc/sysconfig/iptables”. DHCP-palvelimien vikasietoisuuden toimimisen kannalta palomuurisääntö, joka sallii liikenteen ensisijaisen ja toissijaisen palvelimen välillä, on hyvin tärkeä. Centos1-palvelimeen määritelty palomuurisääntö, joka varmistaa sen, että vikasietoisuus centos1:n ja centos2:n välillä tulee toimimaan on seuraava.

```
-A INPUT -p tcp -s 172.31.31.40 --dport 647 -d 172.31.31.30 -j ACCEPT
```

Centos2-palvelimen iptables-säännöissä IP-osoitteet ovat kyseisen säännön kohdalla määritelty toisinpäin. Säännöllä sallitaan TCP-liikenne porttiin 647 tietystä lähdeosoitteesta, joka yllä olevassa centos1:n palomuurisäännössä on centos2:n osoite 172.31.31.40. Kohdeosoitteena on centos1:n osoite.

DHCP-palvelimen toimimiseksi piti sallia yhteys UDP-portteihin 67 ja 68. Tämä tapahtui seuraavilla säännöillä.

```
-A INPUT -p udp --dport 67 -j ACCEPT
-A INPUT -p udp --dport 68 -j ACCEPT
```

DNS-palvelimen toiminta vastaavasti vaati sen, että yhteys UDP- ja TCP-portteihin 53 sallittiin. Lisäksi testiympäristössä sallittiin ICMP echo (tyyppi 8), joka tarkoitti käytännössä sitä, että ping-komennot toimivat testiympäristössä. Näin ollen oli mahdollista varmistaa yhteyksien toiminta testivaiheissa. Nämä määritykset tehtiin seuraavilla palomuurisäännöillä.

```
-A INPUT -p tcp --dport 53 -j ACCEPT
-A INPUT -p udp --dport 53 -j ACCEPT
-A INPUT -p icmp --icmp-type 8 - j ACCEPT
```

NTP-palvelun toimimiseksi palomuurisäännöissä sallittiin UDP-yhteys portista 123. Testiympäristön toiminnan kannalta yllä luetellut säännöt ovat tärkeimpiä. Palomuurisääntöjä on kuitenkin mainittujen lisäksi myös muita ja ne selviävät liitteestä 1, jossa on listattu centos1-palvelimen kaikki palomuurisäännöt. Centos2-palvelimen palomuurisäännöt ovat kaikkien sääntöjen osalta samanlaiset paitsi tässä luvussa ensimmäiseksi mainitun säännön osalta.

Liite 1 selventää myös IPv6-palomuurisäännöt, jotka määriteltiin tiedostossa ”/etc/sysconfig/ip6tables”. Tärkeimpiä IPv6-palomuurisääntöjä testiympäristön toiminnan kannalta ovat säännöt, jotka mahdollistavat DHCP- ja DNS-palvelimien toiminnan. Nämä säännöt ovat seuraavat.

```
-A INPUT -p udp --dport 547 -j ACCEPT
-A INPUT -p tcp --dport 53 -j ACCEPT
-A INPUT -p udp --dport 53 -j ACCEPT
```

Säännöt sallivat UDP-yhteyden porttiin 547, joka on DHCPv6-palvelimen käyttämä portti. Vastaavasti kuin IPv4-palomuurisäännöissä piti IPv6-palomuurisäännöissä sallia yhteydet DNS-palvelimen käyttämään porttiin 53.

Palomuurisääntöjen konfiguroimisen jälkeen piti iptables- ja ip6tables-palvelut käynnistää uudestaan. Tämä tapahtui komennoilla "service iptables restart" ja "service ip6tables restart".

6.4.3 DHCP-palvelimen asentaminen

DHCP-palvelin asennettiin ensin toimimaan IPv4:n kanssa. Tämä alkoi ISC DHCP -palvelinohjelmiston asentamisella molempiin palvelimiin komennolla ”yum install dhcp -y”. ISC DHCP -ohjelmistoa käytettiin myöhemmin myös DHCPv6:n käyttöönotossa. Asentamisen jälkeen tiedostoon ”/etc/sysconfig/dhcpd” muokattiin tieto siitä, missä verkkoliitännässä DHCP on käytössä. Tämä määritys oli testiverkossa "DHCPDARGS=eth0". DHCP-palvelimen konfiguroiminen tapahtui tiedostossa ”/etc/dhcp/dhcpd.conf”. Centos1-palvelin konfiguroitiin konfiguraatiotiedostossa ensisijaiseksi (primary) ja centos2 omassa konfiguraatiossaan toissijaiseksi (secondary). Kommunikointi kahden palvelimen välillä tapahtui portilla 647. Vikasietoisuus on toteuttu failover-tekniikalla. Ensisijaisen palvelimen vikaantuessa, toissijainen palvelin alkaa jakamaan samaa osoitealuetta. Centos1:n konfiguraatiotiedosto löytyy liitteestä 2 ja centos2:n liitteestä 3.

DHCP-konfiguraatioissa varsinkin testauksen kannalta on tärkeä määritys "log-facility local1;". Tällä määrityksellä DHCP-loki tallennetaan omaan tiedostoonsa. Tiedosto, johon loki tallennetaan, määritetään tiedostossa "/etc/rsyslog.conf",

jonka loppuun on lisätty rivi "local1.* /var/log/dhcpd.log". Lisäksi lokitiedosto pitää luoda komennolla "touch /var/log/dhcpd.log" ja palvelu käynnistää uudelleen komennolla "service rsyslog restart". Luodun lokitiedoston lisäksi tiedosto "/var/log/messages" on hyvä apu virheiden etsimisessä testausvaiheessa.

DHCP-palvelu käynnistettiin molemmilla palvelimilla komennolla "service dhcpd start". Komento, jolla palvelu saadaan käynnistymään automaattisesti palvelimen käynnistyksen yhteydessä oli "chkconfig --levels 235 dhcpd on".

DHCPv6:n konfiguroiminen tapahtui tiedostossa "/etc/dhcp/dhcpd6.conf". Tiedostoon määriteltiin seuraavia yleisiä asetuksia.

```
authoritative;
option dhcp6.name-servers 2001:708:410:3::30, 2001:708:410:3::40;
option dhcp6.domain-search "inside.lpt.fi";
ddns-update-style none;
update-static-leases off;
```

Authoritative-määritys määrittää käytettävän DHCPv6-palvelimen valtuutetuksi. Option-määrityksissä määritetään nimipalvelimien IPv6-osoitteet ja toimialue. Rivi "ddns-update-style none;" määrittää sen, että dynaamisia DNS-päivityksiä ei DHCPv6:ssa oteta käyttöön kuten ei alkuperäisessä IPv4-toteutuksessa otettu. Suunnitelma koski julkista langatonta verkkoa, joten nimi- ja IP-parien muodostaminen asiakaskoneista ei ole tarpeellista. Myöskään staattisia osoitteita ei päivitetä. Lisäksi konfiguraatiossa määritettiin osoitteiden eliniät. Preferred-eliniäksi määriteltiin testiverkossa kaksi tuntia ja valid-eliniäksi 4 tuntia. Nämä määritykset tapahtuivat seuraavilla riveillä.

```
default-lease-time 14400;
preferred-lifetime 7200;
```

Jaettava osoitealue määriteltiin DHCPv6:ssa seuraavalla tavalla.

```
subnet6 2001:708:410:3::/64 {
        range6 2001:708:410:3::41 2001:708:410:3::200;
}
```

Lisäksi DHCPv6-konfiguraatiossa määritettiin asetus DHCPv6-tapahtumien tallentamiseksi omaan lokitiedostoon. Konfiguraatiotiedoston rivin lisäksi

tiedostoon "/etc/rsyslog.conf" piti lisätä tiedostosta oma rivi samalla tavalla kuin oli tehty IPv4 DHCP -lokin kanssa. Ennen kuin lokit tallentuivat, piti lokitiedosto luoda ja rsyslog-palvelu käynnistää uudelleen. DHCPv6:n konfiguraatio löytyy kokonaisuudessaan liitteestä 4.

DHCPv6:lle on olemassa myös failover-protokolla, mutta ISC DHCP ei tukenut sitä vielä työn toteutusvaiheessa. Näin ollen vikasietoisuutta ei DHCPv6:lle voitu toteuttaa samalla tavalla kuin IPv4:n DHCP:n kanssa. DHCPv6:n kanssa vikasietoisuuden voi kuitenkin toteuttaa samalla tavalla kuin Windows-palvelimilla eli toinen palvelin laitetaan jakamaan eri osoitealuetta kuin ensimmäinen palvelin jakaa. Tätä ei kuitenkaan toteutettu testiympäristössä, koska se ei poikkea centos1-palvelimen DHCPv6-palvelimen käyttöönottotavasta.

DHCPv6-palvelun käynnistys tapahtui komennolla "service dhcpd6 start". Jotta myös DHCPv6-palvelu käynnistyy palvelimen käynnistyksen yhteydessä automaattisesti, annettiin komento "chkconfig --levels 235 dhcpd6 on".

Huomioitavaa CentOS-palvelimien DHCPv6 toteutuksen testaamisessa oli se, että testikone sai IPv6-osoitteen, mutta ei pystynyt pingaamaan palvelimia. Tämä johtui siitä, että DHCPv6:ssa ei ole mahdollista mainostaa reittiä asiakaskoneelle. Näiden RA-viestien (Router Advertisement) välittäminen olisi testiympäristön mukaisessa verkossa ollut pfSensen tehtävä. pfSense oli kuitenkin jätetty pois IPv6-testauksesta. Tämän vuoksi DNS:n testaamisen aikana testikoneeseen määritettiin käsin IPv6-osoite 2001:708:410:3::/64-verkosta ja DNS-palvelimien osoitteet 2001:708:410:3::30 (centos1) ja 2001:708:410:3::40 (centos2).

6.4.4 DNS-palvelimen asentaminen

Vikasietoisen DNS-palvelimen toteutus alkoi asentamalla palvelimiin BIND-nimipalvelinohjelmisto komennolla "yum -y install bind-chroot". Palvelu asennettiin chroot-ympäristöön alkuperäisen toteutuksen mukaisesti. Toteutusympäristöksi oli alun perin valittu chroot tietoturvan parantamiseksi. Asennuksen jälkeen määritettiin käyttöoikeudet kuntoon nimipalvelun kansioille komennolla "chmod 755 /var/named/chroot/var/named". Komennolla kyseiselle kansiolle tulee pääkäyttäjälle ja käyttäjäryhmälle täydet oikeudet.

Nimipalvelimen konfiguroiminen tapahtui tiedostossa "/var/named/chroot/etc/named.conf". Tiedostoa ei testiympäristössä ollut kyseisessä sijainnissa, joten se luotiin. Tiedosto koostuu DNS-palvelun asetuksista ja zone-määrityksistä. Asetukset määrittävät nimipalvelun hakemiston, kuunneltavat osoitteet, verkot, joista kyselyt on sallittu ja käytetäänkö rekursiivisia nimipalvelukyselyitä. Alkuperäisessä toteutuksessa zone-tiedot oli jaettu omiin view-alueisiin. Koska tämän työn toteutuksen oli tarkoitus jatkaa alkuperäinen toteutus IPv6-yhteensopivaksi, toteutettiin zone-tiedot kolmeen eri view-alueeseen. Nämä olivat localhost, servers ja hosts. Localhost käsitti palvelimen loopback-osoitteen, servers DMZ-verkon ja hosts LAN-verkon. Zone-määrityksissä kerrotaan onko kyse master- vai slave-palvelimesta ja mikä on käytettävä tiedosto. Lisäksi aluemäärityksiin kuuluu ensisijaisessa DNS-palvelimessa, master-palvelimessa, rivi, jossa kerrotaan sallitaanko alueen siirto toiselle palvelimelle. Slave-palvelimessa vastaavasti on rivi, joka kertoo master-palvelimen osoitteen. Ensisijaisen DNS-palvelimen asetukset selviävät liitteestä 5 ja toissijaisen liitteestä 6.

DNS-konfiguraatiotiedoston asetuksiin piti IPv6:n osalta määrittää kuunneltava IPv6-osoite. Lisäksi verkosta 2001:708:410:3::/64 piti sallia nimikyselyt ja pääsy toimialueisiin (match-clients-määritys). Verkolle 2001:708:410:3::/64 piti myös tehdä servers-alueen alle määritys käänteisiä nimikyselyitä varten. Tämä tehtiin seuraavalla tavalla.

```
zone ”3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa” {
        type master;
        file ”data/3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa”;
        allow-transfer { 172.31.31.40; };
};
```

Molemmista DNS-palvelimista piti löytyä konfiguraatiotiedoston lisäksi kolme tiedostoa. Nämä olivat localhost.zone, named.local ja named.root. Kahta ensimmäistä tiedostoa tarvitaan loopback-yhteyksiä varten. Kolmas tiedosto, named.root, sisältää juuripalvelimien tiedot. Tiedostot kopioitiin BIND -ohjelmiston esimerkkitiedostoista. Testiympäristön CentOS-palvelimen BIND-tiedostoista ei löytynyt localhost.zone-tiedostoa, joten tämä toteutettiin käsin.

Tiedostojen kopiointi oikeaan sijaintiin tapahtui kahden tiedoston kohdalla seuraavilla komennoilla.

```
cp /usr/share/doc/bind-9.8.2/sample/var/named/named.ca
/var/named/chroot/var/named/named.root

cp /usr/share/doc/bind-9.8.2/sample/var/named/named.localhost
/var/named/chroot/var/named/named.local
```

Tiedostot nimettiin eri nimisiksi alkuperäisen toteutuksen mukailun vuoksi. Kyseessä olivat kuitenkin samat tiedostot kuin alkuperäisessä ympäristössä. Käsin toteutetun tiedoston localhost.zone sisältö selviää liitteestä 7.

Verkon toimialueiden zone-tiedostot toteutettiin ainoastaan ensisijaiselle palvelimelle kansioon "/var/named/chroot/var/named/". Servers- ja host-toimialueille tehtiin zone-tiedostot servers.zone ja hosts.zone sekä 31.31.172.zone ja 1.168.192.zone -tiedostot käänteisiä kyselyjä varten. Lisäksi IPv6-verkolle 2001:708:410:3::/64 toteutettiin zone-tiedosto 3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa käänteisiä kyselyjä varten. IPv6:n osalta luotiin lisäksi servers-verkon zone-tiedostoon AAAA-tietueita. Muita muutoksia IPv6 ei aiheuttanut DNS-palvelimen konfiguraatioihin. Testiympäristössä käytetyt zone-tiedostot löytyvät kokonaisuudessaan liitteistä 8 ja 9.

IPv6-toteutuksen kannalta oleellisimpia tiedostoja olivat servers.zone ja käytetyn IPv6-verkon käänteisiin kyselyihin vastaava tiedosto. Tiedoston servers.zone määritykset olivat seuraavat.

```
$ORIGIN inside.lpt.fi.
$TTL 12h

@       IN      SOA     ns1.inside.lpt.fi.      admin.inside.lpt.fi. (
                        2013032700              ; Serial
                        2h                      ; Refresh
                        15m                     ; Retry
                        24h                     ; Expire
                        3h )                    ; Minimum TTL

; Nameservers
        IN      NS      ns1.inside.lpt.fi.
        IN      NS      ns2.inside.lpt.fi.

; Servers
```

```
gateway         IN      A       172.31.31.254
centos1         IN      A       172.31.31.30
                IN      AAAA    2001:708:410:3::30
centos2         IN      A       172.31.31.40
                IN      AAAA    2001:708:410:3::40
ns1             IN      A       172.31.31.30
                IN      AAAA    2001:708:410:3::30
ns2             IN      A       172.31.31.40
                IN      AAAA    2001:708:410:3::40
```

Zone-tiedoston alussa määritetään $ORIGIN-määrityksellä se, että toimialue on inside.lpt.fi. $TTL (Time To Live) kertoo tiedoston säilytysajan nimipalvelimen välimuistissa. Alun määrityksistä oleellinen on tiedoston sarjanumeron esittävä kenttä, koska tällä kerrotaan se, milloin tiedosto on päivitetty. Kenttä muodostetaan vuosiluvusta, kuukaudesta, päivästä ja sarjanumero-osasta. Nimipalvelimien määrittämisen jälkeen on nimipalvelun toimimisen kannalta tärkein osa eli nimien ja osoitteiden yhdistäminen. A-tietue yhdistää nimen ja IPv4-osoitteen ja AAAA-tietue yhdistää nimen ja IPv6-osoitteen.

Verkon 2001:708:410:3::/64 käänteisiä nimikyselyjä varten luotu tiedosto on seuraavanlainen.

```
$TTL 12h

@       IN      SOA     ns1.inside.lpt.fi.  admin.inside.lpt.fi. (
                        2013032700          ; Serial
                        2h                  ; Refresh
                        15m                 ; Retry
                        24h                 ; Expire
                        3h )                ; Minimum TTL

; Nameservers
        IN      NS      ns1.inside.lpt.fi.
        IN      NS      ns2.inside.lpt.fi.

0.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa.
IN  PTR  ns1.inside.lpt.fi.
0.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa.
IN  PTR  centos1.inside.lpt.fi.
0.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa.
IN  PTR  ns2.inside.lpt.fi.
0.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa.
IN  PTR  centos2.inside.lpt.fi.
```

Tiedostossa IPv6-osoitteet on merkitty käänteisessä järjestyksessä. $ORIGIN-määrityksellä käänteisten IPv6-osoitteiden merkitsemistapaa on mahdollista yksinkertaistaa. Tämä tapahtuu seuraavalla tavalla.

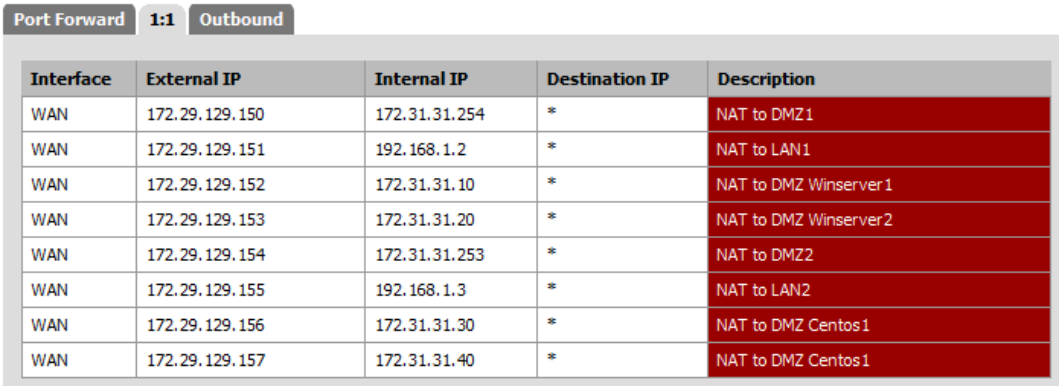
```
$ORIGIN 3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa.
0.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0    IN    PTR    ns1.inside.lpt.fi.
0.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0    IN    PTR    centos1.inside.lpt.fi.
0.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0    IN    PTR    ns2.inside.lpt.fi.
0.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0    IN    PTR    centos2.inside.lpt.fi.
```

DNS-palvelimien konfiguroimisen jälkeen DNS-palvelu käynnistettiin kummassakin palvelimessa komennolla "service named start". Komento "chkconfig --levels 235 named on" saa palvelun käynnistymään automaattisesti palvelimen uudelleen käynnistämisen jälkeen.

6.5 pfSense-palomuuri

Palomuurina toimi pfSense 2.0.1, jonka tarkoitus verkossa oli toimia ulkoverkon ja sisäverkon välillä. Näin ollen palomuuriin oli konfiguroitu DMZ-verkon portin osoitteeksi 172.31.31.254, joka toimi DMZ-alueen laitteiden oletusyhdyskäytävänä. LAN-verkon portin IP-osoitteeksi oli konfiguroitu 192.168.1.1, joka toimi verkon asiakaskoneiden oletusyhdyskäytävänä. WAN-verkon osoite oli konfiguroitu julkisella IP-osoitteella, josta lähti yhteys ulkoverkkoon.

DNS-palvelimien toimintaa varten pfSenseen oli määritelty kuviosta 16 selviävät NAT-asetukset. Jokaiselle testiverkon palvelimelle toteutettiin 1:1-NAT. Tämä tarkoitti sitä, että pfSense määritti palvelimesta ulospäin menevälle liikenteelle oman julkisen IP-osoitteen. Tämä mahdollisti sen, että testiverkossa toimi myös DNS-nimikyselyt ulkoverkon osoitteille.

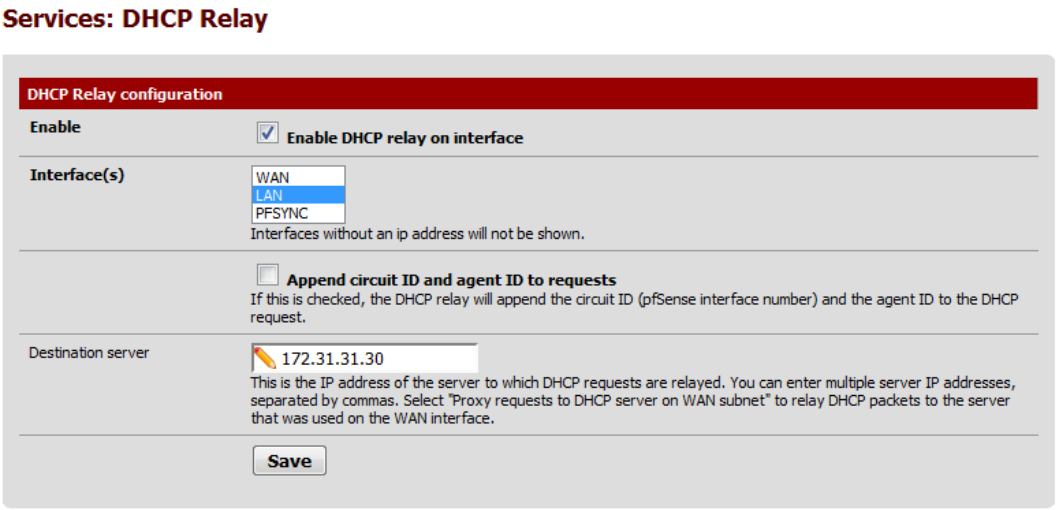


Port Forward | 1:1 | Outbound

Interface	External IP	Internal IP	Destination IP	Description
WAN	172.29.129.150	172.31.31.254	*	NAT to DMZ1
WAN	172.29.129.151	192.168.1.2	*	NAT to LAN1
WAN	172.29.129.152	172.31.31.10	*	NAT to DMZ Winserver1
WAN	172.29.129.153	172.31.31.20	*	NAT to DMZ Winserver2
WAN	172.29.129.154	172.31.31.253	*	NAT to DMZ2
WAN	172.29.129.155	192.168.1.3	*	NAT to LAN2
WAN	172.29.129.156	172.31.31.30	*	NAT to DMZ Centos1
WAN	172.29.129.157	172.31.31.40	*	NAT to DMZ Centos1

KUVIO 16. pfSense-palomuurin NAT-määritykset DMZ-alueen palvelimia varten

DHCP:n toiminnan kannalta oli oleellista se, että pfSenseen oli konfiguroitu DHCP Relay. DHCP Relay -määrityksellä määritettiin se, mihin IP-osoitepyynnöt lähetettiin. pfSenseen oli määritetty testien alkuvaiheessa DHCP Relay -osoitteeksi winserver1-palvelimen osoite. Myöhemmin testattiin myös centos1-palvelimen toiminta laittamalla pfSenseen DHCP Relay -osoitteeksi centos1-palvelimen IP-osoite. pfSensen DHCP Relay -määritykset selviävät kuviosta 17.



KUVIO 17. pfSense-palomuurin DHCP Relay -asetukset

6.6 Windows 7 -testikone

Testikoneeksi asennettiin Windows 7, johon asennuksen jälkeen asennettiin kaikki saatavilla olevat päivitykset. Testikoneen tarkoitus verkossa oli testata DHCP- ja DNS-palvelimien toimintaa. Testauksia varten tarkistettiin, että koneen verkkokortin asetuksista oli IPv4 ja IPv6 määritelty määrittämään osoitteen automaattisesti eli DHCP:tä käyttäen.

Testikoneessa käytettiin työssä ainoastaan komentokehotetta, jolla määritettiin DHCP-palvelimien toimintaa eri testivaiheissa. Komentokehotteella toteutettiin myös DNS-palvelinten toiminnan testaus.

6.7 Testaus

DHCP-palvelinten testaus tapahtui määrittämällä testikone haluttuun verkkoon virtuaalikytkimessä (LAN tai DMZ) ja katsomalla saako testikone DHCP-palvelimelta palvelimeen määritetyt tiedot. DNS-palvelimen toiminta varmistettiin pingaamalla testikoneelta domain-nimiä. Käänteisten nimenselvityspyyntöjen toimimiseksi käytettiin nslookup-komentoa.

Vikasietoisuutta testattiin Windows-palvelimissa DNS-palvelimen osalta ottamalla ensisijaisesta palvelimesta DNS-palvelu pois päältä. Tämä tapahtui palvelimen palveluiden (services) hallinnassa. Mikäli toissijainen palvelin toimi oikein, nimikyselyt onnistuivat testikoneesta myös ensisijaisen palvelimen DNS-palvelun ollessa pois päältä. DHCP:n vikasietoisuutta IPv4:n osalta testattiin vastaavasti ottamalla ensisijaisesta palvelimesta DHCP-palvelu pois päältä. Vikasietoisuus oli siten toteutettu split-scope-ominaisuudella oikein jos testikone sai DHCP-palvelimelta IPv4-osoitteen.

CentOS-palvelimissa DNS-palvelimen vikasietoisuuden testaus tapahtui samalla tavalla kuin Windows-palvelimissa. Ensisijaisesta palvelimesta pysäytettiin DNS-palvelu komennolla "service named stop". Mikäli vikasietoisuus oli toteutettu onnistuneesti, pystyi testikone tekemään nimikyselyjä testin aikana. Lokitiedostoja tarkastelemalla pystyi näkemään, miten ensisijaisen DNS-palvelimen palvelun pysäyttäminen näkyi toissijaisen palvelimen lokeissa. Lokitiedosto, jossa nämä tapahtumat näkyivät oli "/var/log/messages".

CentOS-palvelimien DHCP:n (IPv4) failover-tekniikalla toteutettua vikasietoisuutta testattiin pysäyttämällä ensimmäisestä palvelimesta DHCP-palvelu komennolla "service dhcpd stop". Mikäli vikasietoisuus oli konfiguroitu oikein, alkoi toissijainen palvelin jakamaan osoitteita ensisijaisen palvelimen puolesta. Myös DHCP-palvelimien osalta palvelinten lokimerkintöjä pystyi tarkastelemaan tiedostoista "/var/log/messages" ja DHCP-palvelimen asennusvaiheessa määritellystä tiedostosta "/var/log/dhcpd.log".

6.8 Tulokset

Testien perusteella selvisi, että sekä Windows Server 2008 R2 että CentOS 6.2 -palvelimilla on mahdollista toteuttaa DHCP- ja DNS-verkkopalvelut IPv6-yhteensopiviksi. Niin Windows-ympäristön kuin Linux-ympäristön testauksen aikana testikone sai DHCP-palvelimelta IPv6-asetukset sekä pystyi suorittamaan IPv6-nimikyselyitä DNS-palvelimelta.

Vikasietoisuus oli toteutettavissa kummassakin ympäristössä samalla tavalla DHCPv6-palvelimen osalta eli laittamalla toissijainen palvelin jakamaan eri osoitealuetta. CentOS-palvelinten IPv4:n DHCP:ssä failover-protokollalla toteutettu vikasietoisuus oli toiminnaltaan käytännöllinen. Toteutusvaiheessa ISC DHCP ei tukenut failover-protokollaa DHCPv6:lle. Kun failover-protokolla tulee käyttöön myös DHCPv6-palvelimeen, on se IPv4:n DHCP-palvelimen testauksen perusteella toimiva tapa toteuttaa vikasietoisuus.

DNS-palvelimien osalta vikasietoisuus toimi kummassakin ympäristössä onnistuneesti. Toissijaiset palvelimet kopioivat ensisijaiselta palvelimelta zone-tiedostot ja ensisijaisen DNS-palvelimen ollessa pois päältä, toissijaiset palvelimet vastasivat nimikyselyihin.

Toteutustavoiltaan Windows- ja Linux-ympäristöt erosivat toisistaan huomattavasti sillä, että Windows-palvelimissa oli graafinen käyttöjärjestelmä. Graafisessa ympäristössä DHCP- ja DNS-palveluiden asentaminen käyttöön tapahtui asennusvelhojen avustuksella. Myös palveluiden hallinta oli graafisessa käyttöjärjestelmässä hyvin helppoa, koska manuaalista määrittelyä oli verrattain vähän. Linux-palvelimien konfiguroiminen vaati paljon manuaalista määrittelyä ja

virheitä saattoi syntyä helposti johtuen esimerkiksi kirjoitusvirheistä tai ylimääräisistä merkeistä konfiguraatiotiedostoissa. Vianselvitys oli kuitenkin helppoa palveluiden antamista virheilmoituksista tai palvelimien lokitiedostoista.

Vaikka IPv6-verkkopalveluiden toteuttaminen Windows-palvelinympäristöön tuntui helpommalta, on Linux-palvelinympäristö kuitenkin palvelinkäytössä hallittavuudeltaan laajempi ja selkeämpi. Linux-palvelinympäristö on myös tietoturvan kannalta helpommin hallittavissa kuin Windows-ympäristö. Windows-palvelinympäristö tarjoaa kuitenkin mahdollisuuden IPv6-ominaisuuksien käyttöönotolle. Näin ollen mikäli aikaisempi ympäristö on toteutettu Windows-palvelimilla, on mahdollista ympäristöä kehittää myös IPv6-yhteensopivaksi.

7 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli toteuttaa Lahden ilmaisen langattoman verkon, Mastonetin, virtualisoidut verkkopalvelut toimimaan IPv6-protokollan kanssa. Toteutus tehtiin Linux- ja Windows-palvelinympäristöissä, joita vertailtiin lopuksi keskenään.

Linux-palvelinympäristön toteutuksen pohjana käytettiin Mika Pesosen opinnäytetyön "Virtualisoidut verkkopalvelut" toteutusta. Pesonen suunnitteli työssään ympäristön Mastonetille, jonka toteutusta mukaillen tässä työssä pystytettiin testiympäristö IPv6-protokollan käyttöönoton testaamista varten. Linux-ympäristö koostui kahdesta CentOS 6.2 -palvelimesta, joissa molemmissa oli DHCP- ja DNS-palvelimet. Windows-palvelinympäristön toteutuksessa käytettiin Windows Server 2008 R2 -palvelimia, joihin molempiin asennettiin DHCP- ja DNS-palvelimet.

IPv6-verkkopalveluiden käyttöönotto eli DHCP- ja DNS-palveluiden IPv6-tuki onnistui kummassakin ympäristössä ilman suurempia ongelmia. Palveluiden toimintaa testattiin Windows 7 -testikoneella, joka sai molempien ympäristöjen testien aikana DHCP:ltä tarvittavat tiedot, esimerkiksi IPv6-osoitteen ja DNS-palvelimien osoitteet. Testikone myös onnistui tekemään nimikyselyjä IPv6-osoitteista eli DNS-palvelimet saatiin toimimaan IPv6:n kanssa.

Vikasietoisuus DHCPv6:n osalta ei tarjonnut kummassakaan testiympäristössä samanlaista ratkaisua kuin DHCP:n (IPv4) failover-protokollan vikasietoisuus. Vikasietoisuus on kuitenkin toteutettavissa laittamalla toissijainen palvelin jakamaan eri IPv6-osoitealuetta kuin ensisijainen palvelin. Tätä ei kuitenkaan työssä toteutettu, koska toteutus ei olisi kummassakaan ympäristössä eronnut toissijaisessa palvelimessa ensisijaisen palvelimen toteutuksesta.

Windows-palvelimet tarjosivat toteutukselle graafisen ympäristön. Tämän vuoksi Windows-ympäristössä myös IPv6-ominaisuuksien konfiguroiminen oli Linux-ympäristöön verrattuna helpompaa. Linux-palvelimissa konfiguroiminen vaati huomattavasti enemmän manuaalista määrittelyä. Näin ollen virheiden syntymisen mahdollisuus oli Linux-ympäristössä todennäköisempää. Linux-palvelimissa vianselvitys kuitenkin oli helppoa sen jälkeen, kun virheilmoituksien ja

lokitiedostojen tulkiseminen tuli tutuksi.

Työ onnistui, koska työssä saavutettiin tavoite saada Mastonetin virtualisoidut verkkopalvelut toimimaan IPv6-protokollan kanssa. Toteutus onnistui alkuperäisen toteutuksen Linux-ympäristössä ja vertailtavan toteutuksen Windows-ympäristössä.

Työn perusteella voidaan todeta, että IPv6-ominaisuudet ovat toteutettavissa Windows Server 2008 R2 ja CentOS 6.2 -palvelimilla. Linux-palvelimet ovat tietoturvaominaisuuksiensa vuoksi palvelinkäytössä hyvä ratkaisu. Mikäli aikaisempi ympäristö on toteutettu Windows-palvelimilla, ei IPv6-ominaisuuksien käyttöönoton vuoksi toiseen palvelinympäristöön vaihtaminen ole tarpeellista.

Tämän opinnäytetyön toteutuksen aikana on julkaistu Windows Server 2012. Julkaisu tapahtui syyskuussa 2012. Työ päätettiin kuitenkin toteuttaa loppuun Windows Server 2008 R2 -palvelimilla. Windows Server 2012 tuo IPv6:n osalta kehittyneitä ominaisuuksia, joita ovat muun muassa sisäänrakennetut NAT64- ja DNS64-toteutukset. Windows Server 2012 on näin ollen tutustumisen arvoinen palvelinympäristöä suunnitellessa IPv6-yhteensopivaksi.

IPv4-osoitteet eivät riitä ikuisesti. IPv6 tuo ratkaisun osoitteiden loppumiseen ja antaa mahdollisuuden uusien tekniikoiden kehittämiseen. IPv6:n käyttö tulee yleistymään vaikka protokollan alkutaival onkin ollut vielä hidasta. Käyttöönottoon on hyvä valmistautua ajoissa ja kehittää järjestelmiä IPv6-yhteensopiviksi.

LÄHTEET

Anttila, A. 2000. TCP/IP-tekniikka. Helsinki: Helsinki Media.

van Beijnum, I. 2006. Running IPv6. Yhdysvallat: Springer-Verlag New York, Inc.

Britt, D., Davis, C., Forrester, J., Liu, W., Matthews, C., Parziale, L. & Rosselot, N. 2006. TCP/IP Tutorial and Technical Overview. Yhdysvallat: IBM Corporation.

Cricket, L. 2011. DNS and BIND on IPv6. Yhdysvallat: O'Reilly Media, Inc.

Davies, J. 2012. Understanding IPv6. 3. painos. Yhdysvallat: Microsoft Corporation.

Dostálek, L. & Kabelová, A. 2006. DNS in Action. Olton Birmingham, Iso-Britannia: Packt Publishing Ltd.

Droms, R., Lemon, T. 2003. The DHCP Handbook. 2. painos. Yhdysvallat: Sams Publishing.

Hagen, S. 2006. IPv6 essentials. 2. painos. Yhdysvallat: O'Reilly Media, Inc.

Hagino, J. 2005. IPv6 network programming. Yhdysvallat: Elsevier, Inc.

Heikkilä, J. 2011. Nettiosoitteet loppuvat viikon sisällä - hidastuuko verkko?. MTV3 [viitattu 16.1.2012]. Saatavissa: http://www.mtv3.fi/uutiset/talous.shtml/2011/01/1262493/nettiosoitteet-loppuvat-viikon-sisalla---hidastuuko-verkko.

Kotilainen, S. 2011. Internetin ipv6-päivä onnistui – ei suuria ongelmia. Sanoma Magazines Finland Oy [viitattu 15.3.2013]. Saatavissa: http://www.tietokone.fi/uutiset/internetin_ipv6_paiva_onnistui_ei_suuria_ongelmia.

Kotilainen, S. 2012. Netin jättimuutos tulee kesällä – ongelmia koteihin. Sanoma Magazines Finland Oy [viitattu 15.3.2013]. Saatavissa:

http://www.tietokone.fi/uutiset/netin_jattimuutos_tulee_kesalla_ongelmia_koteihin.

Laitila, T. 2011. Tänään testataan IPv6:n toimivuus. AfterDawn Oy [viitattu 15.3.]. Saatavissa: http://fin.afterdawn.com/uutiset/artikkeli.cfm/2011/06/08/tanaan_testataan_ipv6_n_toimivuus.

Lehto, T. 2011. Tänään IPv6 on tositestissä webissä. Sanoma Magazines Finland Oy [viitattu 15.3.2013]. Saatavissa: http://www.tietokone.fi/uutiset/tanaan_ipv6_on_tositestissa_webissa.

Loshin, P. 2004. IPv6: theory, protocol, and practice. 2. painos. Yhdysvallat: Elsevier, Inc.

Pesonen, M. 2010. Virtualisoidut verkkopalvelut. Lahti: Lahden ammattikorkeakoulu, Tekniikan ala. AMK-opinnäytetyö.

Roivas, P. 2011. IP-osoitteet loppuivat kesken, Internet on täysi. AfterDawn Oy [viitattu 16.1.2012]. Saatavissa: http://fin.afterdawn.com/uutiset/artikkeli.cfm/2011/02/03/ip-osoitteet_loppuivat_kesken_internet_on_taysi.

Youngsong, M. & Hyewon, K. L. 2005. Understanding IPv6. Yhdysvallat: Springer Science+Business Media, Inc.

LIITTEET

LIITE 1. Centos1-palvelimen palomuurisäännöt

```
# /etc/sysconfig/iptables

*filter
:INPUT DROP [6:360]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [6:360]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp --dport 53 -j ACCEPT
-A INPUT -p udp --dport 67 -j ACCEPT
-A INPUT -p udp --dport 68 -j ACCEPT
-A INPUT -p udp --dport 53 -j ACCEPT
-A INPUT -p udp --sport 123 -j ACCEPT
-A INPUT -p tcp --dport 22 -j ACCEPT
-A INPUT -p icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp --icmp-type 3 -j ACCEPT
-A INPUT -p icmp --icmp-type 8 - j ACCEPT
-A INPUT -p icmp --icmp-type 11 -j ACCEPT
-A INPUT -p tcp -s 172.31.31.40 --dport 647 -d 172.31.31.30 -j
ACCEPT
COMMIT
```

```
# /etc/sysconfig/ip6tables

*filter
:INPUT DROP [6:360]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [6:360]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p ipv6-icmp -j ACCEPT
-A INPUT -p tcp --dport 53 -j ACCEPT
-A INPUT -p udp --dport 53 -j ACCEPT
-A INPUT -p udp --dport 547 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp6-adm-prohibited
-A FORWARD -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
```

LIITE 2. Ensisijaisen DHCP-palvelimen IPv4-konfiguraatio

```
# centos1: primary
# /etc/dhcp/dhcpd.conf

authoritative;

ddns-update-style none;
ignore client-updates;

log-facility local1;

failover peer ”failover-dhcp” {
       primary;
       address 172.31.31.30;
       port 647;
       peer address 172.31.31.40;
       peer port 647;
       max-response-delay 30;
       max-unacked-updates 10;
       load balance max seconds 3;
       mclt 1800;
       split 128;
}

subnet 192.168.1.0 netmask 255.255.255.0 {
       option routers  192.168.1.1;
       option subnet-mask 255.255.255.0;
       option broadcast-address 192.168.1.255;

       option domain-name ”inside.lpt.fi”;
       option domain-name-servers 172.31.31.30, 172.31.31.40;

       pool {
              failover peer ”failover-dhcp”;
              deny dynamic bootp clients;
              range 192.168.1.10 192.168.1.254;
              default-lease-time 7200;
              max-lease-time 14400;
       }
}

subnet 172.31.31.0 netmask 255.255.255.0 {
       option routers 172.31.31.254;
       option subnet-mask 255.255.255.0;
       option broadcast-address 172.31.31.255;

       option domain-name ”inside.lpt.fi”;
       option domain-name-servers 172.31.31.30, 172.31.31.40;

       pool {
              failover peer ”failover-dhcp”;
              deny dynamic bootp clients;
                     range 172.31.31.41 172.31.31.254;
                     default-lease-time 7200;
                     max-lease-time 14000;
       }
}
```

LIITE 3. Toissijaisen DHCP-palvelimen IPv4-konfiguraatio

```
# centos2: secondary
# /etc/dhcp/dhcpd.conf

authoritative;

ddns-update-style none;
ignore client-updates;

log-facility local1;

failover peer ”failover-dhcp” {
       secondary;
       address 172.31.31.40;
       port 647;
       peer address 172.31.31.30;
       peer port 647;
       max-response-delay 30;
       max-unacked-updates 10;
       load balance max seconds 3;
}

subnet 192.168.1.0 netmask 255.255.255.0 {
       option routers  192.168.1.1;
       option subnet-mask 255.255.255.0;
       option broadcast-address 192.168.1.255;

       option domain-name ”inside.lpt.fi”;
       option domain-name-servers 172.31.31.30, 172.31.31.40;

       pool {
              failover peer ”failover-dhcp”;
              deny dynamic bootp clients;
              range 192.168.1.10 192.168.1.254;
              default-lease-time 7200;
              max-lease-time 14400;
       }
}

subnet 172.31.31.0 netmask 255.255.255.0 {
       option routers 172.31.31.254;
       option subnet-mask 255.255.255.0;
       option broadcast-address 172.31.31.255;

       option domain-name ”inside.lpt.fi”;
       option domain-name-servers 172.31.31.30, 172.31.31.40;

       pool {
              failover peer ”failover-dhcp”;
              deny dynamic bootp clients;
              range 172.31.31.41 172.31.31.254;
              default-lease-time 7200;
              max-lease-time 14000;
       }
}
```

LIITE 4. Centos1-palvelimen DHCPv6-konfiguraatio

```
# centos1
# /etc/dhcp/dhcpd6.conf

authoritative;

option dhcp6.name-servers 2001:708:410:3::30, 2001:708:410:3::40;
option dhcp6.domain-search "inside.lpt.fi";

ddns-update-style none;
update-static-leases off;

default-lease-time 14400;
preferred-lifetime 7200;

log-facility local2;

subnet6 2001:708:410:3::/64 {
       range6 2001:708:410:3::41 2001:708:410:3::200;
}
```

LIITE 5/1. Ensisijaisen DNS-palvelimen konfiguraatio

```
# centos1
# /var/named/chroot/etc/named.conf

options {
      directory       ”/var/named”;
      listen-on       { 172.31.31.30; };
      listen-on-v6    { 2001:708:410:3::30; };
      allow-query     { 172.31.31.0/24; 192.168.1.0/24;
                      2001:708:410:3::/64; localhost; };
      recursion       yes;
      version         ””;
};

view ”localhost” {
      match-clients   { localhost; };

      zone ”localhost” {
            type master;
            file ”localhost.zone”;
      };
      zone ”0.0.127.in-addr.arpa” {
            type master;
            file ”names.local”;
      };
};

view ”servers” {
      match-clients {  172.31.31.0/24; 192.168.1.0/24;
                       2001:708:410:3::/64; };

      zone ”inside.lpt.fi” {
            type master;
            file ”data/servers.zone”;
            allow-transfer { 172.31.31.40; };
      };
      zone ”31.31.172.in-addr.arpa” {
            type master;
            file ”data/31.31.172.zone”;
            allow-transfer { 172.31.31.40; };
      };
      zone ”3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa” {
            type master;
            file ”data/3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa”;
            allow-transfer { 172.31.31.40; };
      };

};


view ”hosts” {
      match-clients {  172.31.31.0/24; 192.168.1.0/24;
                       2001:708:410:3::/64; };

      zone ”inside.lpt.fi” {
            type master;
            file ”data/hosts.zone”;
            allow-transfer { 172.31.31.40; };
```

LIITE 5/2.

```
        };
        zone ”1.168.192.in-addr.arpa” {
                type master;
                file ”data/1.168.192.zone”;
                allow-transfer { 172.31.31.40; };
        };
};

view ”root” {
        match-clients {  172.31.31.0/24; 192.168.1.0/24;
                         2001:708:410:3::/64};

        zone ”.” {
                type hint;
                file ”named.root”;
        };
};
```

LIITE 6/1. Toissijaisen DNS-palvelimen konfiguraatio

```
# centos2
# /var/named/chroot/etc/named.conf

options {
      directory       ”/var/named”;
      listen-on       { 172.31.31.40; };
      listen-on-v6    { 2001:708:410:3::40; };
      allow-query     { 172.31.31.0/24; 192.168.1.0/24;
                      2001:708:410:3::/64; localhost; };
      recursion       yes;
      version         ””;
};

view ”localhost” {
      match-clients   { localhost; };

      zone ”localhost” {
            type master;
            file ”localhost.zone”;
      };
      zone ”0.0.127.in-addr.arpa” {
            type master;
            file ”names.local”;
      };
};

view ”servers” {
      match-clients {  172.31.31.0/24; 192.168.1.0/24;
                       2001:708:410:3::/64; };

      zone ”inside.lpt.fi” {
            type slave;
            file ”slaves/servers.zone”;
            masters { 172.31.31.30; };
      };
      zone ”31.31.172.in-addr.arpa” {
            type slave;
            file ”slaves/31.31.172.zone”;
            masters { 172.31.31.30; };
      };
      zone ”3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa” {
            type slave;
            file ”data/3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip6.arpa”;
            masters { 172.31.31.30; };
      };
};


view ”hosts” {
      match-clients {  172.31.31.0/24; 192.168.1.0/24;
                       2001:708:410:3::/64; };

      zone ”inside.lpt.fi” {
            type slave;
            file ”slaves/hosts.zone”;
            masters { 172.31.31.30; };
      };
```

LIITE 6/2.

```
      zone ”1.168.192.in-addr.arpa” {
            type slave;
            file ”slaves/1.168.192.zone”;
            masters { 172.31.31.30; };
      };
};

view ”root” {
      match-clients {  172.31.31.0/24; 192.168.1.0/24;
                       2001:708:410:3::/64; };

      zone ”.” {
            type hint;
            file ”named.root”;
      };
};
```

LIITE 7. DNS-palvelinten localhost.zone-tiedosto

```
# /var/named/chroot/var/named/localhost.zone

$TTL 1D

@       IN      SOA     @ rname.invalid. (
                        2013032700      ; Serial
                        1d              ; Refresh
                        1h              ; Retry
                        1w              ; Expire
                        3h )            ; Minimum

        NS      @
        A       127.0.0.1
        AAAA    ::1
```

LIITE 8. DNS-palvelimen zone-tiedostot

```
# /var/named/chroot/var/named/data/servers.zone

$ORIGIN inside.lpt.fi.
$TTL 12h

@       IN      SOA     ns1.inside.lpt.fi.   admin.inside.lpt.fi. (
                        2013032700      ; Serial
                        2h              ; Refresh
                        15m             ; Retry
                        24h             ; Expire
                        3h )            ; Minimum TTL

; Nameservers
        IN      NS      ns1.inside.lpt.fi.
        IN      NS      ns2.inside.lpt.fi.

; Servers
gateway         IN      A       172.31.31.254
centos1         IN      A       172.31.31.30
                IN      AAAA    2001:708:410:3::30
centos2         IN      A       172.31.31.40
                IN      AAAA    2001:708:410:3::40
ns1             IN      A       172.31.31.30
                IN      AAAA    2001:708:410:3::30
ns2             IN      A       172.31.31.40
                IN      AAAA    2001:708:410:3::40
```

```
# /var/named/chroot/var/named/data/hosts.zone

$ORIGIN inside.lpt.fi.
$TTL 12h

@       IN      SOA     ns1.inside.lpt.fi.   admin.inside.lpt.fi. (
                        2013032700      ; Serial
                        2h              ; Refresh
                        15m             ; Retry
                        24h             ; Expire
                        3h )            ; Minimum TTL

; Nameservers
        IN      NS      ns1.inside.lpt.fi.
        IN      NS      ns2.inside.lpt.fi.

; Servers
gateway         IN      A       192.168.1.1
centos1         IN      A       172.31.31.30
centos2         IN      A       172.31.31.40
ns1             IN      A       172.31.31.30
ns2             IN      A       172.31.31.40
```

LIITE 9/1. DNS-palvelimen in-addr.arpa-tiedostot

```
# /var/named/chroot/var/named/data/31.31.172.zone

$ORIGIN 31.31.172.IN-ADDR.ARPA.
$TTL 12h

@       IN      SOA     ns1.inside.lpt.fi.   admin.inside.lpt.fi. (
                        2013032700      ; Serial
                        2h              ; Refresh
                        15m             ; Retry
                        24h             ; Expire
                        3h )            ; Minimum TTL

; Nameservers
        IN      NS      ns1.inside.lpt.fi.
        IN      NS      ns2.inside.lpt.fi.

; Servers
254             IN      PTR     gateway.inside.lpt.fi.
30              IN      PTR     ns1.inside.lpt.fi.
30              IN      PTR     centos1.inside.lpt.fi.
40              IN      PTR     ns2.inside.lpt.fi.
40              IN      PTR     centos2.inside.lpt.fi.
```

```
# /var/named/chroot/var/named/data/1.168.192.zone

$ORIGIN 1.168.192.IN-ADDR.ARPA.
$TTL 12h

@       IN      SOA     ns1.inside.lpt.fi.   admin.inside.lpt.fi. (
                        2013032700      ; Serial
                        2h              ; Refresh
                        15m             ; Retry
                        24h             ; Expire
                        3h )            ; Minimum TTL

; Nameservers
        IN      NS      ns1.inside.lpt.fi.
        IN      NS      ns2.inside.lpt.fi.

; Servers
1               IN      PTR     gateway.inside.lpt.fi.
```

LIITE 9/2.

```
# /var/named/chroot/var/named/data/3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2
.ip6.arpa

$TTL 12h

@       IN      SOA     ns1.inside.lpt.fi.   admin.inside.lpt.fi. (
                        2013032700      ; Serial
                        2h              ; Refresh
                        15m             ; Retry
                        24h             ; Expire
                        3h )            ; Minimum TTL

; Nameservers
        IN      NS      ns1.inside.lpt.fi.
        IN      NS      ns2.inside.lpt.fi.

0.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip
6.arpa.     IN    PTR    ns1.inside.lpt.fi.
0.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip
6.arpa.     IN    PTR    centos1.inside.lpt.fi.
0.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip
6.arpa.     IN    PTR    ns2.inside.lpt.fi.
0.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.1.4.0.8.0.7.0.1.0.0.2.ip
6.arpa.     IN    PTR    centos2.inside.lpt.fi.
```